HERRAMIENTAS PARA LA FORMACIÓN DE
PROFESORES DE MATEMÁTICAS

$$\bigcup \{A,B\} = A \cup B$$

LA TEORÍA DE CONJUNTOS
Y LOS FUNDAMENTOS DE LA MATEMÁTICA

RENATO LEWIN

J·C·SÁEZ editor

La teoría de conjuntos y
los fundamentos de la matemática

ISBN: 978-956-306-065-2
Registro de Propiedad Intelectual: 200.533
Colección: Herramientas para la formación de profesores de matemáticas.
Diseño: Jessica Jure de la Cerda.
Diseño de Ilustraciones: Cristina Felmer Plominsky, Catalina Frávega Thomas.
Diagramación: Pedro Montealegre Barba, Francisco Santibáñez Palma.
Financiamiento: Proyecto Fondef D05I-10211.

Datos de contacto para la adquisición de los libros:
Para Chile:
1. En librerías para clientes directos.
2. Instituciones privadas directamente con:
   Juan Carlos Sáez C.
   Director Gerente
   Comunicaciones Noreste Ltda.
   J.C. Sáez Editor
   jcsaezc@vtr.net
   www.jcsaezeditor.blogspot.com
   Oficina: (56 2) 3260104 - (56 2) 3253148
3. Instituciones públicas o fiscales: www.chilecompra.cl

Desde el extranjero:
1. Liberalia Ediciones: www.liberalia.cl
2. Librería Antártica: www.antartica.cl
3. Argentina: Ediciones Manantial: www.emanantial.com.ar
4. Colombia: Editorial Siglo del Hombre
   Fono: (571) 3377700
5. España: Tarahumara, tarahumara@tarahumaralibros.com
   Fono: (34 91) 3656221
6. México: Alejandría Distribución Bibliográfica, alejandria@alejandrialibros.com.mx
   Fono: (52 5) 556161319 - (52 5) 6167509
7. Perú: Librería La Familia, Avenida República de Chile # 661
8. Uruguay: Dolmen Ediciones del Uruguay
   Fono: 00-598-2-7124857

La teoría de conjuntos y los fundamentos de la matemática | Renato Lewin
Facultad de Matemáticas, Pontificia Universidad Católica de Chile
rlewin@mat.puc.cl

ESTA PRIMERA EDICIÓN DE 2.000 EJEMPLARES
Se terminó de imprimir en febrero de 2011 en WORLDCOLOR CHILE S.A.

Derechos exclusivos reservados para todos los países. Prohibida su reproducción total o parcial, para uso privado o colectivo, en cualquier medio impreso o electrónico, de acuerdo a las leyes N°17.336 y 18.443 de 1985 (Propiedad intelectual). Impreso en Chile.

LA TEORÍA DE CONJUNTOS Y LOS FUNDAMENTOS DE LA MATEMÁTICA

Renato Lewin

Pontificia Universidad Católica de Chile

Editores

Patricio Felmer, Universidad de Chile.
Doctor en Matemáticas, Universidad de Wisconsin-Madison,
Estados Unidos

Salomé Martínez, Universidad de Chile.
Doctora en Matemáticas, Universidad de Minnesota,
Estados Unidos

Comité Editorial Monografías

Rafael Benguria, Pontificia Universidad Católica de Chile.
Doctor en Física, Universidad de Princeton,
Estados Unidos

Servet Martínez, Universidad de Chile.
Doctor en Matemáticas, Universidad de Paris VI,
Francia

Fidel Oteíza, Universidad de Santiago de Chile.
Doctor en Currículum e Instrucción, Universidad del Estado de Pennsylvania,
Estados Unidos

Dirección del Proyecto Fondef D05I-10211
Herramientas para la Formación de Profesores de Matemática

Patricio Felmer, Director del Proyecto
Universidad de Chile.

Leonor Varas, Directora Adjunta del Proyecto
Universidad de Chile.

Salomé Martínez, Subdirectora de Monografías
Universidad de Chile.

Cristián Reyes, Subdirector de Estudio de Casos
Universidad de Chile.

Presentación de la Colección

La colección de monografías que presentamos es el resultado del generoso esfuerzo de los autores, quienes han dedicado su tiempo y conocimiento a la tarea de escribir un texto de matemática. Pero este esfuerzo y generosidad no se encuentra plenamente representado en esta labor, sino que también en la enorme capacidad de aprendizaje que debieron mostrar, para entender y comprender las motivaciones y necesidades de los lectores: Futuros profesores de matemática.

Los autores, encantados una y otra vez por la matemática, sus abstracciones y aplicaciones, enfrentaron la tarea de buscar la mejor manera de traspasar ese encanto a un futuro profesor de matemática. Éste también se encanta y vibra con la matemática, pero además se apasiona con la posibilidad de explicarla, enseñarla y entregarla a los jóvenes estudiantes secundarios. Si la tarea parecía fácil en un comienzo, esta segunda dimensión puso al autor, matemático de profesión, un tremendo desafío. Tuvo que salir de su oficina a escuchar a los estudiantes de pedagogía, a los profesores, a los formadores de profesores y a sus pares. Tuvo que recibir críticas, someterse a la opinión de otros y reescribir una y otra vez su texto. Capítulos enteros resultaban inadecuados, el orden de los contenidos y de los ejemplos era inapropiado, se hacía necesario escribir una nueva versión y otra más. Conversaron con otros autores, escucharon sus opiniones, sostuvieron reuniones con los editores. Escuchar a los estudiantes de pedagogía significó, en muchos casos, realizar eventos de acercamiento, desarrollar cursos en base a la monografía, o formar parte de cursos ya establecidos. Es así que estas monografías recogen la experiencia de los autores y del equipo del proyecto, y también de formadores de profesores y estudiantes de pedagogía. Ellas son el fruto de un esfuerzo consciente y deliberado de acercamiento, de apertura de caminos, de despliegue de puentes entre mundos, muchas veces, separados por falta de comunicación y cuya unión es vital para el progreso de nuestra educación.

La colección de monografías que presentamos comprende una porción importante de los temas que usualmente encontramos en los currículos de formación de profesores de matemática de enseñanza media, pero en ningún caso pretende ser exhaustiva. Del mismo modo, se incorporan temas que sugieren nuevas formas de abordar los contenidos, con énfasis en una matemática más pertinente para el futuro profesor, la que difiere en su enfoque de la matemática para un ingeniero o para un licenciado en matemática, por ejemplo. El formato de monografía, que aborda temas específicos

con extensión moderada, les da flexibilidad para que sean usadas de muy diversas maneras, ya sea como texto de un curso, material complementario, documento básico de un seminario, tema de memoria y también como lectura personal. Su utilidad ciertamente va más allá de las aulas universitarias, pues esta colección puede convertirse en la base de una biblioteca personal del futuro profesor o profesora, puede ser usada como material de consulta por profesores en ejercicio y como texto en cursos de especialización y post-títulos. Esta colección de monografías puede ser usada en concepciones curriculares muy distintas. Es, en suma, una herramienta nueva y valiosa, que a partir de ahora estará a disposición de estudiantes de pedagogía en matemática, formadores de profesores y profesores en ejercicio.

El momento en que esta colección de monografías fue concebida, hace cuatro años, no es casual. Nuestro interés por la creación de herramientas que contribuyan a la formación de profesores de matemática coincide con un acercamiento entre matemáticos y formadores de profesores que ha estado ocurriendo en Chile y en otros lugares del mundo. Nuestra motivación nace a partir de una creciente preocupación en todos los niveles de la sociedad, que ha ido abriendo paso a una demanda social y a un interés nacional por la calidad de la educación, expresada de muy diversas formas. Esta preocupación y nuestro interés encontró eco inmediato en un grupo de matemáticos, inicialmente de la Universidad de Chile, pero que muy rápidamente fue involucrando a matemáticos de la Pontificia Universidad Católica de Chile, de la Universidad de Concepción, de la Universidad Andrés Bello, de la Universidad Federico Santa María, de la Universidad Adolfo Ibáñez, de la Universidad de La Serena y también de la Universidad de la República de Uruguay y de la Universidad de Colorado de Estados Unidos.

La matemática ha adquirido un rol central en la sociedad actual, siendo un pilar fundamental que sustenta el desarrollo en sus diversas expresiones. Constituye el cimiento creciente de todas las disciplinas científicas, de sus aplicaciones en la tecnología y es clave en las habilidades básicas para la vida. Es así que la matemática actualmente se encuentra en el corazón del currículo escolar en el mundo y en particular en Chile. No es posible que un país que pretenda lograr un desarrollo que involucre a toda la sociedad, descuide el cultivo de la matemática o la formación de quienes tienen la misión de traspasar de generación en generación los conocimientos que la sociedad ha acumulado a lo largo de su historia.

Nuestro país vive cambios importantes en educación. Se ha llegado a la convicción que la formación de profesores es la base que nos permitirá generar los cambios cualitativos en calidad que nuestra sociedad ha impuesto. Conscientes de que la tarea formativa de los profesores de matemática y de las futuras generaciones de jóvenes es extremadamente compleja, debido a que confluyen un sinnúmero de factores y disciplinas, a través de esta colección de monografías, sus editores, autores y todos los que han participado del proyecto en cada una de sus etapas, contribuyen a esta tarea, poniendo a disposición una herramienta adicional que ahora debe tomar vida propia en los formadores, estudiantes, futuros profesores y jóvenes de nuestro país.

Patricio Felmer y Salomé Martínez
Editores

Agradecimientos

Agradecemos a todos quienes han hecho posible la realización de este proyecto Fondef: "Herramientas para la formación de Profesores de Matemáticas". A Cristián Cox, quien apoyó con decisión la idea original y contribuyó de manera crucial para obtener la participación del Ministerio de Educación como institución asociada. Agradecemos a Carlos Eugenio Beca por su apoyo durante toda la realización del proyecto. A Rafael Correa, Edgar Kausel y Juan Carlos Sáez, miembros del Comité Directivo. Agradecemos a Rafael Benguria, Servet Martínez y Fidel Oteiza, miembros del Comité Editorial de la colección, quienes realizaron valiosos aportes a los textos. A José Sánchez, entonces Decano de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Concepción, quién contribuyó de manera decisiva a lograr la integridad de la colección de 15 monografías y a Jaime San Martín, director del Centro de Modelamiento Matemático por su apoyo durante toda la realización del proyecto. Agradecemos a Víctor Campos, Ejecutivo de Proyectos de Fondef, por su colaboración y ayuda en las distintas etapas del proyecto.

En este volumen manisfestamos nuestro especial agradecimiento a Guillermo Marshall, quién fuera Decano de la Facultad de Matemáticas de la Pontificia Universidad Católica de Chile cuando iniciamos este proyecto. Su apoyo decidido y generoso permitió que esta monografía sea parte de la colección. Más aún, su convicción sobre la importancia del involucramiento de matemáticos en la educación y el sentido nacional que esto tiene, fue un importante aliciente en la concreción de las tareas que el proyecto demandó.

Agradecemos también a Bárbara Ossandón de la Universidad de Santiago, a Jorge Ávila de la Universidad Católica Silva Henríquez, a Víctor Díaz de la Universidad de Magallanes, a Patricio Canelo de la Universidad de Playa Ancha en San Felipe y a Osvaldo Venegas y Silvia Vidal de la Universidad Católica de Temuco, quienes hicieron posible las visitas que realizamos a las carreras de pedagogía en matemática. Agradecemos a todos los evaluadores, alumnos, académicos y profesores -cuyos nombres no incluimos por ser más de una centena- quienes entregaron sugerencias, críticas y comentarios a los autores, que ayudaron a enriquecer cada uno de los textos.

Agradecemos a Marcela Lizana por su impecable aporte en todas las labores administrativas del proyecto, a Aldo Muzio por su colaboración en la etapa de evaluación, y también a Anyel Alfaro por sus contribuciones en la etapa final del proyecto y en la difusión de los logros alcanzados.

Dirección del Proyecto

Índice General

Prefacio 17

Capítulo 1: Teoría Intuitiva y Teoría Axiomática de Conjuntos 21

1.1 Operaciones básicas 21
1.2 Productos Cartesianos 32

Capítulo 2: Sistemas Numéricos 57

2.1 Los Números Naturales 57
2.2 Los Números Enteros 74
2.3 Los Números Racionales 82
2.4 Los Números Reales 91

Capítulo 3. Cardinalidad 103

3.1 Conjuntos infinitos 105

Capítulo 4. Teoría Axiomática de Conjuntos 117

4.1 ¿Qué es una Teoría Axiomática? 117
4.2 Los Axiomas de Zermelo Fraenkel I 119
4.3 Los Axiomas de Zermelo Fraenkel II 121
4.4 El Axioma de Elección 126
4.5 APENDICE A: Equivalencias del Axioma de Elección: Demostraciones 133
4.6 APENDICE B: Formalización 138

Bibliografía 141
Índice Analítico 143

Prefacio

Entre las décadas de los 60 y los 80 del siglo pasado, los conjuntos tuvieron un gran protagonismo en la educación pre–universitaria. La verdad es que, más allá de una indudable ayuda para facilitar la expresión de conceptos en forma compacta, no hay ninguna rama de la matemática en donde la teoría de conjuntos sea imprescindible para el desarrollo de la misma. Por otra parte, la enseñanza de los conjuntos en la escuela se ha circunscrito a la exposición del lenguaje de la teoría, pero nunca, ni siquiera en los cursos de nivel universitario, se llega a tocar sus verdaderos problemas y objetivos. Esto es, en algún sentido, afortunado, porque estos son altamente técnicos, especializados y presuponen un nivel de abstracción muy avanzado, el ciudadano común no los necesita y tienden más bien a confundirlo que a aclarar conceptos más concretos. Hoy día es ampliamente aceptado que su introducción, a través del movimiento "new math", produjo un desastre en la enseñanza de la matemática.

La introducción de estos conceptos a través de profesores que no la conocían bien, presentó una idea equivocada acerca de qué es esta disciplina. La creencia común, incluso entre los matemáticos profesionales no especialistas, es que la teoría de conjuntos se trata de una formalización rigurosa de conceptos como relaciones, funciones, etc., junto a una suerte de álgebra sobre estos objetos llamados conjuntos, donde las operaciones son uniones, intersecciones y complementos. La verdad es que esos son aspectos muy superficiales y que poco o nada tienen que ver con el fondo del asunto, se trata más bien de requisitos para desarrollar ideas más de fondo.

La teoría de conjuntos es una maravillosa y profunda rama de la matemática que busca proporcionar una base lógicamente sólida en la cual fundar esta disciplina. Como ocurre con la mayoría de las empresas intelectuales, con el correr de los años la teoría de conjuntos desarrolló temas y planteó problemas propios que no están directamente relacionados con el proyecto fundacional.

La teoría de conjuntos se puede estudiar al menos en tres dimensiones:

1. Como un lenguaje útil para expresar la mayoría de los conceptos matemáticos.
2. Como el contexto adecuado para fundar la matemática.
3. Como tema de investigación dentro de la matemática, similar a la teoría de probabilidades, la teoría de grupos, las ecuaciones diferenciales, etc.

Como explicamos anteriormente, la primera es útil pero no necesaria y puede ser aprendida transversalmente en los distintos cursos de matemática, como parte del lenguaje técnico. La tercera es un tema de especialización para investigadores, adecuado más que nada en fases finales de una licenciatura en matemáticas o en el postgrado. La segunda dimensión es entonces la más atractiva y útil para personas que necesiten una sólida formación matemática, como es el caso de los profesores de la disciplina.

Este libro se ha pensado como un texto guía para un curso de teoría de conjuntos para escuelas formadoras de profesores de matemática de Enseñanza Media. En él se abordan las primeras dos dimensiones. La primera forma parte del lenguaje técnico estándar que tiene que manejar todo matemático y en particular los profesores. Esto es lo que durante años se enseñó en los colegios y universidades como *Teoría de Conjuntos*, pero si no es estudiada a la luz de una teoría axiomática, no tiene mayor contenido; podría tratarse en un apéndice de cualquiera de las monografías: la de Álgebra, Geometría u otra.

El problema de los fundamentos de la matemática es un tema que todo profesor debería conocer. La mayoría de los matemáticos adquiere estos conocimientos "por aquí y por allá" en forma no sistemática, generalmente sin dedicarle atención al meollo del problema de los fundamentos, que no es otro que justificar la existencia y funcionamiento de todos los objetos y conceptos que define dentro de un marco lógicamente adecuado. Este libro intenta satisfacer este segundo enfoque sin uso de herramientas de lógica formal. Para ello se debe prestar atención especial a garantizar permanentemente que los objetos definidos; funciones, relaciones, pares ordenados, números naturales, enteros, etc., sean conjuntos dentro de la teoría.

Una segunda característica formal de este texto es que se presentan demostraciones completas y detalladas de la gran mayoría de los resultados. Sin embargo, no es su propósito introducir al lector a la Lógica Matemática, no suponemos que éste sepa lógica más allá de los conocimientos que se aprenden en un curso universitario de Álgebra. Dado el nivel de abstracción del tema, el libro supone que este es un curso terminal en la carrera, cuando el alumno tiene mayor madurez tanto conceptual como en la fluidez de las demostraciones. Usaremos, por lo tanto, un estilo semiformal el que, por un lado, es habitual en el tema y, por el otro, no apabulla al lector con un rigor tedioso y excesivo.

En el primer capítulo se estudian los conceptos elementales de la teoría de conjuntos. Es importante insistir que, si bien puede ser un complemento para ese fin, este no es un texto para aprender los conceptos de unión, intersección, diagramas de Euler–Venn, relación, función, gráficos, composiciones de funciones y un largo etcétera, tal como aparecen en libros de Introducción al Álgebra o similares. Supondremos que el lector ya los conoce, que domina su operatoria, sus aplicaciones y que está en

condiciones de reflexionar acerca de ellos. La revisión de estos conceptos se hace desde la óptica de una teoría axiomática, en la que lo más importante es que el lector se dé cuenta de la necesidad de contar con axiomas que garanticen la existencia de los conjuntos y construcciones realizadas para justificar su coherencia lógica. Insistimos que sin esta reflexión, la teoría no pasa de ser un lenguaje especializado útil pero prescindible, por este motivo no hacemos un repaso exhaustivo de todas las propiedades de estos conceptos sino sólo de los esenciales para los contenidos posteriores, desarrollados en los siguientes dos capítulos. Tampoco hay ejercicios de aplicación al cálculo o al álgebra. De acuerdo con el enfoque adoptado, los ejercicios apropiados para este tema son esencialmente iguales a los teoremas que están detalladamente demostrados en el texto.

La teoría de conjuntos no termina aquí sino todo lo contrario, es a partir de este punto que podemos comenzar a desarrollar la teoría propiamente tal.

En el segundo capítulo se construye rigurosamente los conjuntos de números dentro de la teoría de Zermelo–Fraenkel. Se presta especial cuidado en garantizar la existencia de cada objeto mediante los axiomas. Es muy importante que el alumno comprenda que estos conjuntos son un modelo abstracto dentro de la teoría de conjuntos, pero no se pretende que sean "los números", lo que quiera que estos sean. En el mismo espíritu de lo dicho para el capítulo anterior, este no es un texto para aprender teoría de números o propiedades de los números reales, el lector debe conocer eso de antemano. El capítulo culmina con la construcción de los números reales mediante cortaduras de Dedekind, que es lo más apropiado dentro de una teoría de conjuntos.

En el tercer capítulo se estudia otra aplicación de la teoría de conjuntos, a saber, el concepto de cardinalidad de un conjunto, en particular el concepto de conjunto infinito. Se muestra cómo hay cardinales infinitos más y más grandes. Mediante el teorema de Cantor–Bernstein se presenta una manera fácil de comparar cardinalidades. Este sí es un contenido que muy probablemente los lectores no habrán estudiado anteriormente y en él se presentan algunos ejercicios más aplicados.

El cuarto capítulo es de naturaleza distinta y de un mayor grado de dificultad. En él se presentan todos los axiomas de la teoría de conjuntos según la clásica formalización de Zermelo–Fraenkel. Esto tiene dos objetivos, el primero es presentar una teoría axiomática. El segundo es dar un marco más riguroso al tratamiento semiformal usado en los capítulos anteriores. Especial mención merece el axioma de elección por su importancia dentro de la matemática. Dada la dificultad relativa de la demostración de las proposiciones equivalentes con el axioma de elección, ésta se reserva para una sección final optativa. Una dificultad adicional de ésta es que no es posible proponer muchos ejercicios porque la mayoría está fuera del nivel de profundidad de este libro. El apéndice sobre estas demostraciones escapa con mucho al nivel de profundidad

que se pretende alcanzar en esta obra y ha sido incluido sólo porque es un material muy difícil de encontrar en castellano y podría interesar a algunos lectores que deseen profundizar en el tema.

El libro puede ser usado como texto guía o texto complementario para un curso de teoría de conjuntos o como texto para una parte de un programa más general de fundamentos de la matemática. Por su naturaleza, este curso debería estar al final de la carrera de profesor de matemática, probablemente como optativo de profundización. Como texto de un curso, puede usarse de varias maneras.

La primera forma es estudiar el libro tal como está escrito, salvo quizás por alterar el orden de los capítulos 2 y 3 que son independientes entre sí.

La segunda forma es leer simultáneamente los capítulos 1 y 4 y proseguir con los otros dos capítulos en cualquier orden. Se me ha sugerido reescribir el libro fundiendo estos dos capítulos, a lo cual presté especial consideración, esa es probablemente la manera más común de presentar la teoría. He preferido usar la estructura actual porque hace una presentación más liviana de la teoría axiomática, de suyo difícil y con aspectos tediosos.

Una tercera forma de hacer un curso, o una parte de él, es estudiar el primer capítulo, luego el último y después estudiar las aplicaciones a los fundamentos de los Capítulos 2 y 3.

Cualquiera sea la manera de usar el libro, insistimos en que el lector debe conocer la teoría intuitiva desarrollada desde la perspectiva axiomática en el Capítulo 1. Sugiero que el lector que no tenga suficientemente maduros estos conocimientos, complemente la lectura del Capítulo 1 con algún texto elemental (por ejemplo, los conocidos textos de la colección Schaum), de manera que pueda desarrollar las intuiciones básicas a través de ejemplos concretos allí presentados.

El autor agradece a José Aguayo, Patricio Felmer, Salomé Martínez, Aníbal Medina, Jaime San Martín, Gloria Schwarze y Xavier Vidaux, así como también a varios lectores anónimos, profesores y alumnos de pedagogía en matemática, quienes hicieron numerosas correcciones y comentarios y otras mejoras al manuscrito original.

Capítulo 1: Teoría Intuitiva y Teoría Axiomática de Conjuntos

La Teoría de los Conjuntos es la base, el lenguaje, de los Fundamentos de la Matemática.

La Teoría de Conjuntos tiene su origen en la preocupación por los fundamentos de la matemática en la segunda mitad del siglo XIX. En los dos siglos anteriores la matemática había tenido un desarrollo explosivo y hasta entonces no había surgido la necesidad de preocuparse por el aparataje lógico que la sustenta. Sin embargo, la creciente complejidad conceptual del siglo XIX llamó la atención sobre posibles dificultades. Georg Cantor, a quien se atribuye la paternidad de la teoría de conjuntos, desarrolló sus ideas a partir de conjuntos de números que aparecían en sus trabajos sobre series trigonométricas.

Al trabajo de Cantor se le ha dado el nombre de *Teoría Intuitiva de Conjuntos* porque intentaba formalizar las nociones que tenían entonces los matemáticos acerca de las colecciones de objetos matemáticos, las funciones y de los mismos números. Esa porción de la teoría es lo que habitualmente se aprende como Teoría de Conjuntos en las escuelas primarias, secundarias y universitarias. Como veremos en este capítulo, esa teoría intuitiva se vio enfrentada a serias dificultades ya que, tal como estaba formulada, era inconsistente. Sin embargo, la idea ya estaba lanzada y muchos matemáticos buscaron la manera de mejorar la presentación. Entre ellos destacan B. Russell y E. Zermelo. La solución más aceptada es la propuesta por este último, a saber, formular una teoría axiomática lógicamente correcta. En este primer capítulo revisaremos esas intuiciones, que son aquellas que, como dijimos en el Prefacio, suponemos conocidas por el lector, a la luz de la teoría axiomática propuesta por Zermelo.

Comenzaremos haciendo un análisis de las ideas intuitivas de conjunto, de la relación de pertenencia a un conjunto y de las propiedades de estos conceptos, desde la perspectiva de una teoría axiomática, haciendo hincapié en los lugares en donde se necesita de un axioma para justificar la existencia de ciertos conjuntos o construcciones. Más adelante, en el Capítulo 4, haremos una presentación más formal de la teoría axiomática de Zermelo–Fraenkel (ZF).

1.1 Operaciones básicas

Este capítulo trata sobre los conjuntos. Intuitivamente un *conjunto* es una colección (clase, agregado, conglomerado, etc.) de objetos. Decimos que los objetos que conforman un conjunto *pertenecen* a él y también que el conjunto *contiene* dichos objetos.

La Teoría Axiomática de Conjuntos busca describir y estudiar formalmente las intuiciones que tenemos sobre los conjuntos y la relación de pertenencia entre ellos. Como toda teoría axiomática, ella debe partir de conceptos no definidos, aquellos que se quiere abstraer, y de axiomas que los gobiernan. En nuestro caso entonces, los conceptos no definidos son objetos llamados "conjuntos" y una relación binaria entre ellos llamada "pertenencia". Una dificultad que enfrentan los estudiantes, al estudiar una teoría axiomática, es que confunden los objetos "reales" con los objetos "virtuales" que los representan en la teoría axiomática, atribuyéndoles a estos últimos las propiedades y características de los primeros. Por ejemplo, un conjunto "real" es una especie de saco que contiene cosas, a menudo llamadas "elementos", estos elementos son desde luego distintos de los conjuntos que los contienen. Como tales, se les puede agregar o quitar elementos, se les puede comparar, contar, etc. Los conjuntos "virtuales" de la teoría axiomática en cambio son entes no definidos cuyas propiedades están estrictamente limitadas por aquello que queramos que verifiquen, a saber, los axiomas que los rigen. Una buena teoría axiomática, entonces, debe proporcionar a los conjuntos "virtuales" propiedades que se asemejen a aquellas que tienen los conjuntos "reales" que modela.

La relación que existe entre un conjunto x y un conjunto A al cual pertenece, se llama *pertenencia* y se denota[1] $x \in A$. También decimos que A *contiene* a x. Si x no pertenece al conjunto A se denota $x \notin A$.

Es habitual decir que aquellos objetos que pertenecen al conjunto son sus *elementos*. Debe tenerse en claro que un elemento de un conjunto es un conjunto, que a su vez tiene sus propios elementos. Repetimos, todos los objetos de la teoría son conjuntos, llamarle a un conjunto "elemento" es sólo una nomenclatura útil que indica la relación que éste tiene con otro conjunto.

Dada nuestra intuición de que los conjuntos son contenedores de objetos, los objetos que contienen los caracterizan. Adoptaremos el siguiente criterio: todo conjunto de la teoría está determinado por los conjuntos que contiene, es importante, por lo tanto, que al definir un conjunto quede muy claro qué objetos pertenecen y qué objetos no pertenecen a él.

Estas ideas intuitivas tienen una consecuencia inmediata:

Observación 1.1.

1. *Dos conjuntos son iguales si y solamente si tienen los mismos elementos.*
2. *Equivalentemente, si dos conjuntos son distintos, debe haber un elemento que pertenece a uno de ellos pero no al otro.*

Esta caracterización de los conjuntos a través de los elementos que contiene, es el contenido del primer axioma de la teoría de conjuntos, llamado el Axioma de

[1]El símbolo $\in$ es una estilización de la letra griega ε. Fue introducida por G. Peano para abreviar la palabra $\grave{\varepsilon}\sigma\tau\grave{\iota}$, que significa "es", en griego.

Extensionalidad. En la página 119 del Capítulo 4 hay una formulación del axioma. Aquí sólo hacemos notar que se precisa de un axioma para establecer esta propiedad.

Por ejemplo, un conjunto puede estar formado por los números 1, 2 y 3. Denotaremos este conjunto $\{1, 2, 3\}$. En general, un conjunto formado por un número pequeño de objetos, se denota por una lista de éstos, separados por comas y encerrada entre llaves "{" y "}".

Dado que un conjunto queda determinado por los objetos que contiene, el orden en la lista y las repeticiones no cuentan, de tal manera que $\{a, b\}$, $\{b, a\}$ $\{a, b, a\}$ son tres maneras de denotar a un mismo conjunto, a saber, el conjunto cuyos únicos elementos son los conjuntos a y b.

Hay conjuntos que no pueden describirse con una lista, ya sea porque son infinitos o porque son de difícil descripción.

Es más o menos inmediato ver que a cada conjunto corresponde una propiedad, es decir, aquello que caracteriza a sus elementos, por ejemplo, al conjunto formado por los números $1, 2, \ldots, 98, 99$, le corresponde la propiedad "ser número entero mayor que cero y menor que cien". A la inversa, nuestra intuición nos dice que a toda propiedad o predicado le debe corresponder un conjunto, la colección de todos los conjuntos que verifican dicha propiedad. Para estos usamos la siguiente notación:

$$\{x : x \text{ tiene tal y cual propiedad}\}.$$

En el ejemplo anterior una posible propiedad sería,

$$\{x : x \text{ es un número entero mayor que cero y menor que cien}\}.$$

Esta notación fue introducida por G. Cantor en 1878.

Temprano en el desarrollo de la teoría de conjuntos se descubrió que esta intuición conduce a contradicciones y que debe descartarse. A comienzos del siglo pasado, en 1902, el matemático inglés Bertrand Russell dio con la siguiente paradoja.[2] Veamos cuál es el problema. Si aceptamos que toda propiedad define un conjunto, podemos considerar el conjunto R definido por "un objeto pertenece al conjunto R si y solo si no pertenece a sí mismo". En símbolos

$$R = \{x : x \notin x\}.$$

La pregunta entonces es, ¿pertenece R a R? Si la respuesta es afirmativa, entonces R debe verificar la propiedad que define a R, a saber, $R \notin R$. Por otra parte, si la respuesta es negativa, entonces por definición de R, $R \in R$. En cualquier caso obtenemos la contradicción

$$R \in R \quad \text{si y solo si} \quad R \notin R\,,$$

lo que es obviamente inaceptable. Esta contradicción, conocida como la paradoja de Russell, nos dice que el concepto de "propiedad" es más delicado de lo que suponemos

[2]Cabe señalar que esta paradoja, conocida como la Paradoja de Russell, no es la primera que se descubrió en el contexto de la teoría intuitiva de conjuntos. Burali–Forti y el mismo Cantor habían encontrado problemas con anterioridad. Estos son más técnicos y no los discutiremos en este libro.

y que definitivamente no debe corresponder a lo que llamamos un conjunto. Debemos tomar medidas para evitar que esta paradoja y ninguna otra[3] se produzca en nuestra teoría.

Grosso modo, el criterio adoptado para evitar este tipo de contradicciones consiste en limitar nuestra intuición a conjuntos definidos por elementos que ya pertenecen a un conjunto dado de U, al que en este libro llamaremos *conjunto de referencia*. De esta manera, nuestro esquema básico de definición de conjunto a partir de una propiedad se restringe a considerar sólo objetos que pertenezcan a ese conjunto de referencia. Así, para definir apropiadamente un conjunto debemos reemplazar $\{x : x \text{ tiene tal y cual propiedad}\}$ por

$$C = \{x \in U : x \text{ tiene tal y cual propiedad}\}. \qquad (*)$$

Es interesante ver cómo se evita ahora la paradoja de Russell. En efecto, consideremos $R = \{x \in U : x \notin x\}$ y tratemos de reconstruir la paradoja. Vemos que es perfectamente aceptable afirmar que $R \notin R$, ya que si bien R cumple con la propiedad prescrita, para que R pertenezca a R debe tenerse además que R pertenezca al conjunto de referencia U, si esto no es así, no hay ninguna contradicción.

Para la práctica matemática esta limitación es muy menor, ya que una vez que hayamos construido los objetos matemáticos habituales: números, conjuntos de números, funciones, etc., como conjuntos de la teoría, siempre trabajamos dentro de un conjunto de referencia conocido, por ejemplo, el conjunto de los números reales, el conjunto de todas las funciones de variable compleja, etc.

Como regla general entonces, si definimos como en $(*)$ una colección C de objetos mediante una cierta propiedad[4] y vemos que cada elemento de esta colección pertenece a algún conjunto U previamente definido, entonces esa colección es un conjunto ya que U actúa como conjunto de referencia dentro del cual C ha sido definido. Podemos de ahí en adelante decir que C es un conjunto. Nuevamente enfrentamos la necesidad de un axioma que nos diga que este procedimiento para definir conjuntos es aceptable. Este es el contenido del Axioma de Separación que se puede consultar en la página 119 del Capítulo 4. El nombre del axioma proviene de pensar que la propiedad "separa" o distingue, aquellos conjuntos que pertenecen al conjunto de referencia que la poseen.

Cualquier objeto formado de esa manera es un conjunto. Sin embargo, veremos que hay otros conjuntos que no pueden formarse de esa manera. Para ellos necesitamos axiomas especiales. El próximo párrafo describe el primer caso.

---

[3]Para más información sobre paradojas lógicas el lector puede consultar, por ejemplo, [**13**].

[4]Para no recargar esta presentación, la noción de propiedad se ha dejado en el terreno de lo intuitivo, sin embargo, dentro de la teoría es de vital importancia. En el APÉNDICE B damos una definición más rigurosa de qué debemos entender por *propiedad* dentro de la Teoría Axiomática de conjuntos.

1.1.1 El conjunto vacío

Uno de los objetos matemáticos que produce más confusiones a los no iniciados es el conjunto vacío, a saber, un conjunto que no tiene ningún elemento. Este es una consecuencia inesperada del Axioma de Separación. En efecto, consideremos, por ejemplo, el siguiente conjunto

$$\{x \in U : \ x \neq x\},$$

donde U es un conjunto cualquiera. Es claro que ningún conjunto puede verificar esa condición, por lo que este conjunto no tiene ningún elemento.

El lector cuidadoso debería ponerse receloso. Para definir el conjunto vacío supusimos que hay un conjunto U, ¿cómo sabemos que existe siquiera un conjunto? Su recelo no es exagerado, la existencia de siquiera un conjunto debe estar garantizada por un axioma. El axioma estándar para este efecto es el Axioma del Conjunto Vacío, que presentamos en la página 120, el que dice exactamente eso,

"existe un conjunto que no tiene elementos".

De los párrafos anteriores se desprende que, en presencia del Axioma de Separación, podemos reemplazar el Axioma del Conjunto Vacío por otro axioma que diga "existe un conjunto U" y construir el conjunto vacío como hicimos anteriormente.

Podría argumentarse que éste es sólo un defecto más de nuestra noción intuitiva de conjunto, sin embargo, no es así. El conjunto vacío aparece frecuentemente en la práctica matemática, aunque en un comienzo no lo sepamos. Por ejemplo, se nos pide el conjunto S de todos los números enteros cuyo cuadrado es menor que -10, o el de las raíces reales de la ecuación $4x^2 - x + 3$. En ambos casos, S es el conjunto vacío.

Más adelante veremos otros motivos que nos indican que es deseable contar con un conjunto que no tiene elementos.

Por último, es fácil ver que existe un único conjunto vacío. En efecto, si hubiese dos conjuntos vacíos distintos, en virtud de la observación 1.1, 2, tendría que haber un elemento que pertenece a uno de ellos pero no al otro, pero como ambos son vacíos, esto no es posible. La unicidad del conjunto vacío nos permite denotarlo por un símbolo, a saber, $\emptyset$. [5]

1.1.2 Subconjuntos

Decimos que un conjunto A es un *subconjunto* del conjunto B, si todos los elementos de A pertenecen a B. Esto lo denotamos[6] $A \subseteq B$. Observemos que

Observación 1.2. *Para que A no sea subconjunto de B debe haber un elemento de A que no pertenece a B.*

En tal caso escribimos $A \nsubseteq B$.

[5] Aunque no es relevante para nada relacionado con la teoría, hacemos notar que el símbolo $\emptyset$ no es la letra griega ϕ, como habitualmente se dice, sino que corresponde a la vocal Ø, una "o" cerrada de algunos idiomas escandinavos. Aparentemente fue introducido por A. Weil en 1939.

[6] Aparentemente esta notación fue introducida por Schröder en 1890.

Ejemplos 1.1.

1. $\{1,2\} \subseteq \{1,2,3,4\}$. Obsérvese que $\{1,2\} \notin \{1,2,3,4\}$.
2. En general, si $a \in A$, entonces $\{a\} \subseteq A$ y viceversa.
3. Las relaciones de pertenencia y de ser subconjunto no son mutuamente excluyentes. Consideremos, por ejemplo, $A = \{1, \{1\}\}$, es decir, A es un conjunto con dos elementos, uno de ellos es el número 1 y el otro es el conjunto cuyo único elemento es el número 1. Entonces $\{1\} \in A$, porque es uno de sus elementos. Por otra parte, $\{1\} \subseteq A$ ya que el elemento de $\{1\}$ pertenece a A.
4. Resulta inmediato que $A \subseteq A$, para cualquier conjunto A.
5. Aunque hay que pensarlo un poco más, es también fácil ver que $\emptyset \subseteq A$, para cualquier conjunto A. Argumentamos por contradicción. Si no lo fuera, es decir, si suponemos que $\emptyset \not\subseteq A$, por la observación anterior, debería existir un elemento en $\emptyset$ que no pertenece a A, pero como esto es imposible, debe ser cierto que $\emptyset \subseteq A$.

Dado un conjunto A, podemos imaginar todos sus subconjuntos o partes y reunirlos en un sólo conjunto. Este conjunto lo denotamos $\mathcal{P}(A)$ y se llama el *conjunto potencia* de A,

$$\mathcal{P}(A) = \{x : x \subseteq A\}.$$

Notemos que esta construcción no corresponde al esquema en el que se aplica el Axioma de Separación, ya que no contamos con un conjunto de referencia apropiado, de hecho, para garantizar la existencia del conjunto potencia de un conjunto se necesitará un axioma, el Axioma del Conjunto Potencia. Éste está formulado en la página 121 del Capítulo 4.

1.1.3 Pares

Si tenemos varios objetos, es intuitivo formar una bolsa cuyo contenido es precisamente esos objetos. La verdad es que basta con poder definir el conjunto formado por dos conjuntos A y B, denotado:

$$\{A, B\}.$$

Este es un conjunto cuyos únicos elementos son los conjuntos A y B y se denomina el *par no ordenado* A, B.

Si los dos conjuntos A y B pertenecen a un conjunto de referencia U, entonces el par $\{A, B\}$ se puede definir como $\{x \in U : x = A \text{ o bien } x = B\}$, usando el Axioma de Separación, (la propiedad sería "$x = A$ o bien $x = B$"). Sin embargo, no siempre podemos garantizarlo y surge la necesidad de un nuevo axioma, el Axioma de Pares que aparece en la página 120 del Capítulo 4.

Es claro que $\{A, B\} = \{B, A\}$ porque ambos tienen los mismos elementos. De aquí el nombre de par no ordenado. Por otra parte, A y B no tienen por qué ser distintos. El "par" $\{A, A\}$ se escribe simplemente $\{A\}$ y se le denomina conjunto *singleton* A.

1.1.4 La unión de dos conjuntos

Si tenemos dos bolsas con objetos, resulta natural pensar en combinarlas en una sola. Esta intuición queda capturada por la operación de unión de dos conjuntos. La *unión* de dos conjuntos A y B, denotada $A \cup B$, es el conjunto cuyos elementos son tanto los de A como los de B. En notación más compacta,

$$A \cup B = \{x : x \in A \text{ o bien } x \in B\}.$$

Para garantizar su existencia necesitamos del Axioma de Uniones que aparece en la página 120 en el Capítulo 4.

Nuevamente hacemos notar que si supiéramos que todos los conjuntos que pertenecen a A y los que pertenecen a B pertenecen además a un conjunto U, que tomamos como conjunto de referencia, entonces $A \cup B$ se puede definir como $\{x \in U : x \in A \text{ o bien } x \in B\}$ usando el Axioma de Separación, (la propiedad sería "$x \in A$ o bien $x \in B$"). La necesidad del nuevo axioma está en que no podemos garantizar la existencia de tal U.

Por ejemplo, combinando uniones con pares de conjuntos podemos formar el conjunto

$$\{A_1, A_2, A_3\} = (\{A_1\} \cup \{A_2\}) \cup \{A_3\}.$$

Observe que ambos lados de la igualdad contienen los mismos elementos. Iterando este proceso podemos construir el conjunto que contiene a todos los conjuntos $A_1, A_2, \ldots, A_n$.

$$\{A_1, A_2, \ldots, A_n\} = (\cdots(\{A_1\} \cup \{A_2\}) \cup \cdots \cup \{A_n\}).$$

1.1.5 La intersección de dos conjuntos.

Dadas dos colecciones de objetos, podríamos estar interesados en agrupar todos aquellos que pertenecen a ambas colecciones. Esta intuición es capturada por la operación de intersección de conjuntos. La *intersección*[7] de dos conjuntos A y B, denotada por $A \cap B$, es el conjunto cuyos elementos son aquellos que pertenecen tanto a A como a B. En notación más compacta,

$$A \cap B = \{x \in A : x \in B\}.$$

Observe que para este conjunto no necesitamos un nuevo axioma porque su existencia está garantizada por el Axioma de Separación. Basta con los Axiomas de Separación y de Uniones.

Si los conjuntos A y B no tienen elementos en común, entonces $A \cap B = \emptyset$. Decimos entonces que A y B son *disjuntos*.

Éste es otro motivo por el cual resulta conveniente contar con el conjunto vacío, si no existiera, antes de hablar de la intersección de dos conjuntos, deberíamos verificar si ellos comparten un elemento o no.

[7] Los símbolos $\cup$ y $\cap$ fueron introducido por H. Grassmann en 1844. Más tarde fueron adoptados y popularizados por G. Peano en 1888.

1.1.6 Uniones e intersecciones generalizadas

Las uniones e intersecciones de dos conjuntos pueden generalizarse a tres, cuatro, hasta infinitos conjuntos. En efecto, la unión de dos conjuntos es aquel conjunto que contiene exactamente a los elementos ya sea de uno o del otro (o de ambos). Si tenemos muchos conjuntos, tiene sentido preguntarse por el conjunto que contiene a todos los elementos que están en alguno de esos conjuntos. De la misma manera, tiene sentido preguntarse por aquellos elementos que están en todos los conjuntos considerados. De hecho, el Axioma de Uniones, en la página 120 del Capítulo 4, establece que dado un conjunto A, existe el conjunto formado por los elementos de los elementos de A.

Si A es un conjunto definimos su unión como sigue.

$$\bigcup A = \{x : x \in a \text{ para algún } a \in A\},$$

y si $A \neq \emptyset$, la intersección de A es

$$\bigcap A = \{x : x \in a \text{ para todo } a \in A\}.$$

Luego de un momento de reflexión vemos que es claro que estos dos conjuntos son exactamente lo que dijimos arriba, contiene los elementos de los elementos de A. Observe que A puede ser finito o infinito y la definición es la misma.

Hacemos notar que estas definiciones son mucho más sencillas de lo que parece, en efecto,

$$x \in \bigcup A \quad \text{si y solo si } x \in a \in A, \text{ para algún } a \in A,$$

y por su parte

$$x \in \bigcap A \quad \text{si y solo si } x \in a \in A, \text{ para todo } a \in A.$$

Hemos abreviado $x \in a$ y $a \in A$ por medio de $x \in a \in A$.

Ejemplos 1.2.

1. Consideremos $A = \{\{1,2,3\},\{1,3,5\},\{1,2,4,5\},\{1,2,5\}\}$. Entonces
$$\bigcup A = \{1,2,3,4,5\} \quad \text{y} \quad \bigcap A = \{1\}.$$
2. En general
$$\bigcup\{A,B\} = A \cup B \quad \text{y} \quad \bigcap\{A,B\} = A \cap B.$$
3. Dados dos conjunto a y b, $a \in \bigcup(\bigcup b)$ si existen conjuntos x e y tales que
$$a \in x \in y \in b.$$
4. Es probable que el lector se haya encontrado con conjuntos indexados por un conjunto de índices, por ejemplo, para cada i número natural, tenemos un conjunto A_i. Podemos formar la unión y la intersección de todos ellos.
$$\bigcup_{i\in\mathbb{N}} A_i = \bigcup\{A_i : i \text{ es un número natural }\},$$

y la intersección de A es

$$\bigcap_{i\in\mathbb{N}} A_i = \bigcap\{A_i : i \text{ es un número natural }\}.$$

Este tipo de operaciones es muy útil en distintas ramas de la matemática.

1.1.7 La diferencia de dos conjuntos

Dados dos conjuntos A y B, podemos formar otro conjunto que contiene a aquellos elementos de A que no pertenecen a B. Esta operación se llama convenientemente la *diferencia* entre A y B y se la denota $A - B$ (en muchos textos se usa la notación $A\backslash B$). Corresponde a

$$A - B = \{x \in A \ : \ x \notin B\}.$$

Notemos que no necesitamos un nuevo axioma para construir este conjunto ya que su existencia está garantizada por el Axioma de Separación. El conjunto de referencia es el conjunto A y la propiedad es "$x \notin B$".

1.1.8 El complemento de un conjunto

Cuando trabajamos dentro de un conjunto de referencia U y $A \subseteq U$, aquellos elementos del conjunto de referencia que no pertenecen a A, es decir el conjunto

$$A^c = \{x \in U : x \notin A\},$$

se denomina el complemento relativo de A con respecto a U. Es claro que si el conjunto de referencia cambia, también cambiará el complemento de A, por eso es un complemento relativo al conjunto de referencia. Como veremos en el Capítulo 4, el complemento absoluto, es decir, la colección de todos los objetos (de cualquier conjunto de referencia), que no pertenecen a A, no puede ser un conjunto.

1.1.9 Algunas propiedades algebraicas

Los siguientes teoremas nos dan las propiedades de las operaciones de unión, intersección y diferencia de conjuntos.

Teorema 1.3. Álgebra de Conjuntos.
Para todo conjunto A, B, C se tiene

1. *Asociatividad*
   $A \cup (B \cup C) = (A \cup B) \cup C, \qquad A \cap (B \cap C) = (A \cap B) \cap C,$
2. *Conmutatividad*
   $A \cup B = B \cup A, \qquad A \cap B = B \cap A,$
3. *Idempotencia*
   $A \cup A = A, \qquad A \cap A = A,$
4. *Absorción*
   $A \cup (A \cap B) = A, \qquad A \cap (A \cup B) = A,$

5. *Existencia de neutro*
   $A \cup \emptyset = A, \qquad A \cap \emptyset = \emptyset,$
6. *Distributividad*
   $A \cup (B \cap C) = (A \cup B) \cap (A \cap C), \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$
7. *Leyes de De Morgan*
   $A - (B \cup C) = (A - B) \cap (A - C), \qquad A - (B \cap C) = (A - B) \cup (A - C),$
8. $A - A = \emptyset$;
9. $A = (A \cap B) \cup (A - B)$.

Demostración. Ejercicio. Estas propiedades son consecuencia directa de propiedades lógicas. □

El concepto de subconjunto, se relaciona con las otras operaciones como sigue.

Teorema 1.4. *Para conjuntos A, B, C y D de un conjunto de referencia U, valen las siguientes afirmaciones:*

1. $A \cap B \subseteq A$ *y* $A \cap B \subseteq B$.
2. *Si* $C \subseteq A$ *y* $C \subseteq B$, *entonces* $C \subseteq A \cap B$.
3. $A \subseteq B$ *si y solo si* $A \cap B = A$.
4. *Si* $A \subseteq C$ *y* $B \subseteq D$, *entonces* $A \cap B \subseteq C \cap D$.
5. $A \subseteq A \cup B$ *y* $B \subseteq A \cup B$.
6. *Si* $A \subseteq C$ *y* $B \subseteq C$, *entonces* $A \cup B \subseteq C$.
7. $A \subseteq B$ *si y solo si* $A \cup B = B$.
8. *Si* $A \subseteq C$ *y* $B \subseteq D$, *entonces* $A \cup B \subseteq C \cup D$.

Demostración. Estas propiedades son consecuencia directa de propiedades lógicas. Por ejemplo:
1. Si $x \in A \cap B$, entonces $x \in A$ y $x \in B$, en particular, $x \in A$, es decir, todo elemento de $A \cap B$ está en A, o lo que es lo mismo, $A \cap B \subseteq A$. Análogamente se prueba $A \cap B \subseteq B$.
3. Supongamos que $A \subseteq B$. Entonces si $x \in A$ también $x \in B$, luego $x \in A \cap B$, es decir, vemos que $A \subseteq A \cap B$. Por otra parte, por 1, $A \cap B \subseteq A$, por lo tanto, $A \cap B = A$.

Supongamos ahora que $A \cap B = A$. Entonces si $x \in A$, $x \in A \cap B$ y, por lo tanto, $x \in B$, es decir, $A \subseteq B$, que es lo que queríamos demostrar.

El resto de las proposiciones se prueban en forma similar y quedan como ejercicio. □

1.1.10 Ejercicios

1. Determine si A: pertenece a, es subconjunto de, o ni pertenece ni es subconjunto de alguno de los siguientes conjuntos.

   a) $\{\{A\}, A\}$ b) A
   c) $\emptyset \cap A$ d) $\{A\} - \{\{A\}\}$
   e) $\{A\} \cup A$ f) $\{A\} \cup \{\emptyset\}$

2. Demuestre que :
   a) $\bigcup\{\{a,b,c\},\{a,d,e\},\{a,f\}\} = \{a,b,c,d,e,f\}$.
   b) $\bigcap\{\{a,b,c\},\{a,d,e\},\{a,f\}\} = \{a\}$.
   c) $\bigcup\{A\} = A = \bigcap\{A\}$, para todo conjunto A .
   d) $(\bigcap A) \cap (\bigcap B) \neq \bigcap(A \cap B)$.
3. Pruebe que:
   a) Si $A \cap C = \emptyset$, entonces $A \cap (B \cup C) = A \cap B$.
   b) Si $A \cap B = \emptyset$, entonces $A - B = A$.
   c) Si $A \cap B = \emptyset$ y $A \cup B = C$, entonces $A = C - B$.
   d) Si $A \cup B = \emptyset$, entonces $A = \emptyset$ y $B = \emptyset$.
4. ¿Qué relación hay entre $\mathcal{P}(A \cup B)$ y $\mathcal{P}(A) \cup \mathcal{P}(B)$?
5. Pruebe que:
   a) $\bigcup \mathcal{P}(A) = A$.
   b) $A \subseteq \mathcal{P}(\bigcup A)$.
   c) $\{\emptyset\} \in (\mathcal{P}(\mathcal{P}(A)))$, para todo conjunto A .
   d) $\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(A)))$, para todo conjunto A .
   e) Si $\mathcal{P}(A) = \mathcal{P}(B)$, entonces $A = B$.
6. Se define $A + B = (A - B) \cup (B - A)$, para A y B conjuntos. Pruebe que si A, B , C son conjuntos, entonces:
   a) $A + \emptyset = A$
   b) $A + A = \emptyset$
   c) $A + (B + C) = (A + B) + C$
   d) $A \cap (B + C) = (A \cap B) + (A \cap C)$
   e) $A - B \subseteq A + B$
   f) $A = B$ si y solo si $A + B = \emptyset$
   g) Si $A + C = B + C$, entonces $A = B$
   h) $A \cup C = B \cup C$ si y solo si $A + B \subseteq C$
   i) $(A \cup C) + (B \cup C) = (A + B) - C$
7. Para las siguientes afirmaciones, dé una demostración o un contraejemplo:
   a) $(A - B) - C = A - (B - C)$.
   b) Si $A \cap B = A \cap C$, entonces $B = C$.
   c) Si $A \cup B = A \cup C$ y $A \cap B = A \cap C$, entonces $B = C$.
   d) $A - B = (A \cup B) - B = A - (A \cap B)$.
8. Pruebe que la inclusión $\subseteq$ de conjuntos cumple:
   a) $A \subseteq A$ (reflexividad).
   b) Si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$ (antisimetría).

c) Si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$ (transitividad).

9. Si $B \subseteq A$ y $C \subseteq A$, pruebe que $B \subseteq C$ si y solo si $(A - C) \subseteq (A - B)$.
10. Sean B, C, D subconjuntos del conjunto A. Abreviaremos "$A - x$" por "x'". Pruebe o dé un contraejemplo de:
    a) $B \subseteq C$ si y solo si $B \cap C' = \emptyset$.
    b) $B \subseteq C$ si y solo si $B' \cap C = \emptyset$.
    c) $B \subseteq C$ si y solo si $B' \cup C = A$.
    d) $B \subseteq C$ si y solo si $B \cap C' \subseteq B'$.
11. Pruebe o dé un contraejemplo de:
    a) $A \subseteq B \cap C$ si y solo si $A \subseteq B$ y $A \subseteq C$.
    b) $B \cup C \subseteq A$ si y solo si $B \subseteq A$ y $C \subseteq A$.
    c) Si $A \subseteq B \cup C$, entonces $A \subseteq B$ ó $A \subseteq C$.
    d) Si $B \cap C \subseteq A$, entonces $B \subseteq A$ ó $C \subseteq A$.
12. Demuestre todas las afirmaciones que no se demostraron en el Teorema 1.3.
13. Demuestre todas las afirmaciones que no se demostraron en el Teorema 1.4.

1.2 Productos Cartesianos

Los conceptos de par ordenado y de producto cartesiano de conjuntos fueron un gran avance en el desarrollo de la matemática. Ellos fueron necesarios para el desarrollo de la geometría analítica y más elementalmente, para la representación gráfica de expresiones algebraicas. Empezamos por la definición de par ordenado, un conjunto que identifica dos elementos en un cierto orden.

Recordemos que como estamos construyendo la matemática dentro de la teoría de conjuntos, TODO es un conjunto, debemos, por lo tanto, tener especial cuidado de que estas construcciones lo sean. Por otra parte, también queremos que estos conjuntos tengan las propiedades intuitivas de las correspondientes nociones con las que trabaja el matemático.

Dados dos conjuntos a y b, llamamos *par ordenado* a, b, denotado (a, b), al siguiente conjunto.

$$(a, b) = \{\{a\}, \{a, b\}\},$$

a y b se llaman la primera coordenada, (o abscisa), y segunda coordenada (u ordenada), de (a, b), respectivamente. El Axioma de Pares garantiza que para cada a y b, existe el par ordenado (a, b), (o sea, todo par ordenado de conjuntos es un conjunto dentro de nuestra teoría).

En el par no ordenado $\{a, b\}$ no podemos distinguir ambos elementos ya que $\{a, b\} = \{b, a\}$. En cambio, los elementos del par ordenado (a, b) sí son distinguibles, es decir, sabemos cuál es el primero y cuál es el segundo. Este es el contenido del próximo teorema.

Teorema 1.5. *Si* $(a, b) = (c, d)$, *entonces* $a = c$ *y* $b = d$.

Demostración.
Supongamos que $(a,b) = (c,d)$, esto es,

$$\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}.$$

Hay dos casos, el primero de ellos es si $a = b$. De nuestra suposición tenemos que $\{\{a\}\} = \{\{c\},\{c,d\}\}$, y, por lo tanto, $\{a\} = \{c\} = \{c,d\}$, o sea $a = b = c = d$.

El segundo caso es si $a \neq b$. Ahora nuestra suposición produce dos sub–casos. O bien $\{a\} = \{c\}$, o bien $\{a\} = \{c,d\}$.
En el primer sub–caso, tenemos $a = c$, luego

$$\{a,b\} \in \{\{c\},\{c,d\}\} = \{\{a\},\{a,d\}\}$$

y como $a \neq b$, $\{a,b\} \neq \{a\}$, y por lo tanto, $\{a,b\} = \{c,d\}$, luego $a = c$ y $b = d$.
En el segundo sub–caso, $a = c = d$, luego $\{a,b\} \in \{\{a\}\}$, o sea $b = a$, lo que es una contradicción, o sea, este segundo sub–caso no se puede producir.
En cualquier caso, si $(a,b) = (c,d)$, se tiene $a = c$ y $b = d$. □

Podemos ahora definir triples ordenados y, en general, n-tuplas ordenadas de la manera obvia.

$$\begin{aligned}(a,b,c) &= ((a,b),c)\\ (a,b,c,d) &= ((a,b,c),d)\\ &\vdots\\ (a_1,a_2,\ldots,a_n) &= ((a_1,\ldots,a_{n-1}),a_n)\end{aligned}$$

Ejercicio 1.6. Demuestre que si $a \in A$ y $b \in B$, entonces $(a,b) \in \mathcal{P}(\mathcal{P}(A \cup B))$.

Demostración. Observamos primero que $\{a\} \subseteq A \cup B$ y también $\{a,b\} \subseteq A \cup B$, es decir, $\{a\} \in \mathcal{P}(A \cup B)$ y $\{a,b\} \in \mathcal{P}(A \cup B)$, luego $(a,b) = \{\{a\},\{a,b\}\} \subseteq \mathcal{P}(A \cup B)$ y, por lo tanto, $(a,b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. □

Hacemos notar que el ejercicio anterior prueba nuevamente que cada par ordenado es un conjunto

Definición 1.7. Llamaremos *producto cartesiano* de los conjuntos A y B al conjunto

$$A \times B = \{(x,y) \,:\, x \in A \text{ e } y \in B\}.$$

Para verificar que $A \times B$ es un conjunto, notemos que cada $(x,y) \in \mathcal{P}(\mathcal{P}(A \cup B))$, luego

$$A \times B = \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) \,:\, z = (x,y)\ ,\ x \in A \text{ e } y \in B\},$$

es un conjunto por el Axioma de Separación. Si bien esta última descripción de $A \times B$ garantiza que se trata de un conjunto, es muy confusa de leer y, por lo tanto, usaremos la expresión de utilizada en la definición 1.7, que es más transparente.

Podemos también introducir productos cartesianos triples y cuádruples etc., de la manera obvia. Por ejemplo,

$$A \times B \times C = \{(x, y, z) : x \in A\ ,\ y \in B \ \text{ y } \ z \in C\}\,,$$

sin embargo, como no los usaremos en el resto del texto, no lo haremos formalmente, ni probaremos teoremas acerca de ellos.

Algunas propiedades de los productos cartesianos están resumidas en el siguiente teorema.

Teorema 1.8. *Para conjuntos* $A,\ B\ ,\ C\ ,\ D\ ,$

1. $A \times \emptyset = \emptyset \times A = \emptyset$.
2. *Si* $A \subseteq C$ *y* $B \subseteq D$, *entonces* $A \times B \subseteq C \times D$.
3. $A \times (B \cup C) = A \times B \ \cup \ A \times C$.
4. $A \times (B \cap C) = A \times B \cap A \times C$.

Demostración 1. Supongamos que existe $x \in A \times \emptyset$. Entonces $x = (u, v)$, con $u \in A$ y $v \in \emptyset$, pero esto último es una contradicción, luego no puede existir tal x y, por lo tanto, $A \times \emptyset = \emptyset$. Lo mismo ocurre con $\emptyset \times A$.
2. Sea $x = (u, v) \in A \times B$. Entonces $u \in A \subseteq C$ y $v \in B \subseteq D$, es decir, $x = (u, v) \in C \times D$, o sea, $A \times B \subseteq C \times D$.

Los otros ítemes se dejan como ejercicio. □

1.2.1 Relaciones

Entre los objetos matemáticos más comunes están las relaciones. Las relaciones se establecen entre los elementos de un conjunto, cuando algunos de ellos verifican una condición con respecto a otros. Por ejemplo, decimos que dos números enteros x e y están en relación si uno es menor o igual que el otro, lo que denotamos $x \leq y$. Otra relación se establece si x divide a y, lo que denotamos $x|\, y$, etc.

En las secciones anteriores hemos definido una relación entre conjuntos abstractos, la de ser subconjunto. Dos conjuntos están relacionados si uno es un subconjunto de otro. La misma relación de pertenencia es, valga la redundancia, una relación entre conjuntos.

Cuando decimos que tenemos una cierta relación entre elementos de un conjunto, a menudo escribimos: "tal o cuál elemento está relacionado con este otro y éste está relacionado con aquel". Por ejemplo, en la relación de divisibilidad entre números enteros, 2 está relacionado con 6 y con 1000, 8 está relacionado con 8 y con 16 y con 1000, pero 3 no está relacionado con 23.

Esto nos indica que podemos entender las relaciones como conjuntos de pares ordenados. Aquellos pares que, en un cierto orden, verifican la relación están en ese conjunto y aquellos pares que no la verifican no están en el conjunto. En nuestro último ejemplo los pares $(2, 6), (2, 1000), (8, 8), (8, 16)$, y $(8, 1000)$ (¡e infinitos otros!) están en la relación de divisibilidad, pero el par $(3, 23)$ no lo está. La observación anterior motiva que dentro de la teoría de conjuntos las relaciones sean eso, conjuntos

de pares ordenados. Aprovechamos de insistir que no se debe pensar que ésta es la naturaleza ontológica, por así decirlo, de las relaciones. Lo que realmente afirmamos es que dentro de la teoría de conjuntos como modelo formal de la matemática, las relaciones son conjuntos de pares ordenados. Notemos que las relaciones son entonces un tipo particular de conjunto. [8]

Las relaciones no necesariamente se establecen entre pares de objetos, también puede ser entre tres o más objetos. Por ejemplo, entre los puntos de una recta podemos decir que A, B y C están relacionados si A está entre B y C. Por motivos de espacio y de interés matemático, sólo nos referiremos a relaciones binarias, es decir, aquellas que relacionan pares de objetos. La teoría más general trata de relaciones entre cualquier número de conjuntos pero no será estudiada aquí. Más aún, por los mismos motivos, sólo nos preocuparemos en detalle de cierto tipo de relaciones binarias, funciones, relaciones de orden y relaciones de equivalencia. En adelante omitiremos la palabra binaria y hablaremos sólo de relaciones.

Definición 1.9. Dados dos conjuntos A y B, un subconjunto R de $A \times B$ es una *relación*. Hablamos entonces de una relación entre los elementos de A y los de B, o que R es una *relación entre* A y B o una relación de A en B.

Observemos que todo los elementos de una relación son pares ordenados.

Ejemplo 1.10. Sea $R \subseteq A \times B$ una relación. Entonces, cada una de las coordenadas de un par $(a, b) \in R$ pertenece a $\bigcup(\bigcup R)$. Esto es inmediato ya que para $(a, b) \in R$,

$$\{a, b\} \in (a, b) \in R\,,$$

lo que implica por definición de unión generalizada que $\{a, b\} \in \bigcup R$.

Similarmente $a \in \{a, b\} \in \bigcup R$, o sea, $a \in \bigcup(\bigcup R)$. De la misma manera, $b \in \bigcup(\bigcup R)$.

1.2.2 Funciones

El concepto de función es uno de los más importantes en matemática. Intuitivamente, una función es una regla que asigna a cada elemento de un conjunto un único elemento de otro conjunto (no necesariamente distinto). De esta manera toda función establece una relación entre cada elemento de su dominio y un elemento de su recorrido definiéndose así un conjunto de pares ordenados formados por cada elemento del dominio y su imagen bajo la función. En este sentido, dentro de la teoría de conjuntos, las funciones son un tipo de relación. Esto difiere en alguna medida de la práctica matemática, ya que en ésta el concepto de relación tiene una connotación distinta del concepto de función.

[8] En la práctica matemática habitual estamos acostumbrados a tratar relaciones, funciones, sucesiones, etc., como objetos de distinta naturaleza que los conjuntos. Por ejemplo, los números naturales y los números reales son dos conjuntos, pero una función de los naturales en los reales (una sucesión de números reales) no es un conjunto, es otro tipo de ente. No es el caso dentro de nuestra teoría en la que todo es un conjunto.

Definición 1.11. Una relación F es una *función* si y solo si

$$\text{si } (x,y) \in F \text{ y } (x,z) \in F, \text{ entonces } y = z\,.$$

Definimos también el *dominio* de F

$$\text{Dom } F = \{x : (x,y) \in F \text{ para algún } y\},$$

el *recorrido* de F

$$\text{Rec } F = \{y : (x,y) \in F \text{ para algún } x\}\,.$$

Es importante precisar que cada elemento de $\text{Dom}\, R$ y de $\text{Rec}\, R$ pertenece a $\bigcup(\bigcup R)$, por lo tanto, es virtud del Axioma de Separación, tanto el dominio como el recorrido de una función es un conjunto. No lo hemos escrito como corresponde en la definición sólo para alivianar la lectura.

El próximo teorema nos da las principales propiedades del dominio y del recorrido de una función.

Teorema 1.12. *Sean F, G funciones.*

1. $\text{Rec}\,(F \cup G) = \text{Rec}\, F \cup \text{Rec}\, G$.
2. $\text{Dom}\,(F \cap G) \subseteq \text{Dom}\, F \cap \text{Dom} G$.
3. $\text{Rec}\,(F \cap G) \subseteq \text{Rec}\, F \cap \text{Rec}\, G$.
4. *Si $F \subseteq G$, entonces* $\text{Dom}\, F \subseteq \text{Dom}\, G$ *y* $\text{Rec}\, F \subseteq \text{Rec}\, G$.

Demostración. Para demostrar 2, supongamos que $x \in \text{Dom}\,(F \cap G)$. Entonces existe un y tal que $(x,y) \in (F \cap G)$, o sea, $(x,y) \in F$ y $(x,y) \in G$. Pero esto nos dice que $x \in \text{Dom}\, F$ y $x \in \text{Dom}\, G$, o sea, $x \in \text{Dom}\, F \cap \text{Dom}\, G$.

Llama la atención que la inclusión en el otro sentido no sea parte del teorema. Lo que sucede es que no siempre se cumple. Aunque el teorema no lo pide veamos que esto es así. Para ello sólo basta con dar un contraejemplo. Considere las funciones

$$F = \{(0,0)\} \subseteq \{0\} \times \{0\} \qquad \text{y} \qquad G = \{(0,1)\} \subseteq \{0\} \times \{1\}\,.$$

Vemos que $\text{Dom}\,(F \cap G) = \emptyset$, sin embargo, $0 \in (\text{Dom}\, F \cap \text{Dom}\, G) \neq \emptyset$.

Los otros ítemes se dejan como ejercicio. □

Habitualmente se usan las siguientes notaciones.

Definición 1.13.

1. Si F es una función, $\text{Dom}\, F = A$ y $\text{Rec}\, F \subseteq B$ decimos que F es una *función de A en B* y escribimos

$$\begin{aligned} F : A &\longrightarrow B \\ x &\longmapsto F(x)\,, \end{aligned}$$

donde $F(x)$ denota a aquel único conjunto con el que x está relacionado según la función F. Es habitual llamarlo la *imagen de x*. Note que en particular F es una función de $\text{Dom}\, F$ en $\text{Rec}\, F$. Observemos también que el Axioma

de Extensionalidad, (ver Observaciones 1.1), aplicado a las funciones F y G nos dice que

$$F = G \quad \text{si y solo si} \quad \text{Dom } F = \text{Dom } G \text{ y para todo } x\,, \quad F(x) = G(x).$$

2. El conjunto de todas las funciones de A en B se denota
$$^{A}B = \{F \in \mathcal{P}(A \times B) : F \text{ es función de } A \text{ en } B\}\,.$$
3. Una función F se dice *inyectiva* o *uno a uno* si para todo x e y
$$\text{si } x \neq y\,, \text{ entonces } F(x) \neq F(y)\,,$$
es decir, a conjuntos distintos F asigna conjuntos distintos.
4. Una función F de A en B se dice *sobreyectiva* si para todo $y \in B$ existe $x \in A$ tal que $y = F(x)$, es decir, todo elemento de B es asignado a algún elemento del dominio de F.
5. Una función F de A en B se dice *biyectiva* si es inyectiva y sobreyectiva.

Teorema 1.14. *La función F es inyectiva si y solo si para todo x e y*
$$\text{si } F(x) = F(y)\,, \text{ entonces } x = y\,,$$
es decir, si dos conjuntos tienen la misma imagen, son iguales.

Demostración. Este no es sino el contrarrecíproco de la definición y, por lo tanto, equivalente con ella. □

Cabe destacar que la caracterización de la inyectividad que usamos habitualmente en matemática es la dada por este teorema porque, en la práctica, es más fácil de utilizar. Creemos que el concepto intuitivo queda mejor expresado por la definición anterior.

La siguiente es una forma habitual de construir conjuntos en matemática que, sin embargo, no es trivial, de hecho requiere de un axioma especial, el Axioma de Reemplazo, que será presentado en detalle en la página 122 del Capítulo 4.

Teorema 1.15. *Si $C \subseteq A$ y $F : A \longrightarrow B$ es una función, entonces*
$$F[C] = \{F(x) : x \in C\}$$
es un conjunto, llamado la imagen de C por F.

Demostración. Este teorema es un caso particular del Axioma de Reemplazo y la veremos en detalle en el Capítulo 4. □

Hacemos notar que, como en la práctica matemática se denotan los conjuntos por letras mayúsculas y los elementos de los conjuntos por letras minúsculas, no se necesita de esta notación[9] especial. Lo que aquí llamamos $F[C]$ se denota simplemente $F(C)$ y no hay temor de confundirlo con la imagen de C por F ya que difícilmente C, que

[9]En muchos textos de teoría de conjuntos se usa la notación $F^{*}C$ para ese concepto.

es un subconjunto del dominio de F, pertenecerá también al dominio. Sin embargo, en el contexto más general de la teoría de conjuntos, la distinción entre elemento y conjunto al que pertenece es meramente el de la relación en que se encuentran. No distinguir ambas situaciones puede resultar en una ambigüedad. Para ilustrarlo considere el siguiente ejemplo. Sea

$$\begin{aligned} F : \{0,1,\{0,1\}\} &\longrightarrow \{0,1\} \\ 0 &\longmapsto 0 \\ 1 &\longmapsto 1 \\ \{0,1\} &\longmapsto 1\,. \end{aligned}$$

Entonces debemos distinguir entre $F(\{0,1\}) = 1$ y $F[\{0,1\}] = \{F(0), F(1)\} = \{0,1\}$.

Definición 1.16. La *composición* de dos funciones F y G es la función

$$G \circ F = \{(x,y) \,:\, (x,z) \in F \text{ y } (z,y) \in G\,, \quad \text{para algún } z\}$$

De acuerdo con esto, $z = F(x)$ e $y = G(z)$, o sea, $G \circ F(x) = G(F(x))$.

La *inversa* de F es la relación definida por

$$F^{-1} = \{(y,x) \,:\, (x,y) \in F\}.$$

El lector puede comprobar fácilmente que $G \circ F$ así definida es una función. Sin embargo, en general F^{-1} no es una función. Por ejemplo, si $F : \mathbb{R} \longrightarrow \mathbb{R}$ está definida por $F(x) = x^2$, entonces F^{-1} relaciona 1 con 1 y con -1, de tal manera que F^{-1} no es una función.

Por otra parte, es claro que $G \circ F$ y F^{-1} son conjuntos.

Es interesante también notar que los conceptos de composición de funciones e inversa de una función, se pueden aplicar a relaciones obteniéndose respectivamente la relación compuesta y la relación inversa .

El siguiente teorema nos entrega algunas propiedades de las funciones.

Teorema 1.17. *Sean F, G, H funciones, a, b, c conjuntos.*

1. *Si $F \in {}^a b$ y $b \subseteq c$, entonces $F \in {}^a c$.*
2. *Si $F \in {}^a b$ y $G \in {}^b c$, entonces $G \circ F \in {}^a c$.*
3. *La función $F \in {}^a b$ es inyectiva si y solo si para todo c y todo $G \in {}^c a$ y todo $H \in {}^c a$, si $F \circ G = F \circ H$, entonces $G = H$.*
4. *La función $F \in {}^a b$ es sobreyectiva si y solo si para todo c y todo $G \in {}^b c$ y todo $H \in {}^b c$, si $G \circ F = H \circ F$, entonces $G = H$.*

Demostración.
Demostraremos 3. Como es una equivalencia, debemos demostrar ambas direcciones.

($\Rightarrow$)

Supongamos que F es inyectiva. Sean c un conjunto cualesquiera y $G, H \in {}^{c}a$.

Supongamos también que para todo $x \in c$ se tiene $F \circ G(x) = F \circ H(x)$, es decir, $F(G(x)) = F(H(x))$. Como F es inyectiva, se tiene $G(x) = H(x)$.

Pero, además, Dom G = Dom $H = c$ y, por lo tanto, $G = H$.

($\Leftarrow$)

Argumentamos por contradicción. Supongamos que se verifica la afirmación de la derecha y que, sin embargo, F no es inyectiva. Entonces existen $d, e \in a$, tales que $d \neq e$ y $F(d) = F(e)$.

Consideremos el caso particular en que $c = a$ y definamos las funciones constantes $G\,, H \in {}^{a}a$ tales que para todo $x \in a$, $G(x) = d$ y $H(x) = e$.

Entonces para todo x ,

$$F \circ G(x) = F(G(x)) = F(d) = F(e) = F(H(x)) = F \circ H(x),$$

es decir, $F \circ G = F \circ H$, ya que tienen el mismo dominio. Pero por hipótesis, $G = H$, lo que es una contradicción. Luego F es inyectiva.

El resto de las proposiciones queda como ejercicio. □

Teorema 1.18. *Si F , G y H son funciones (o relaciones), entonces*

1. $(H \circ G) \circ F = H \circ (G \circ F)$.
2. $(G \cup H) \circ F = (G \circ F \cup H \circ F)$, *y* $H \circ (G \cup F) = (H \circ G \cup H \circ F)$.
3. $(G \cap H) \circ F \subseteq (G \circ F \cap G \circ H)$, *y* $H \circ (G \cap F) \subseteq (H \circ G \cap H \circ F)$.
4. *Si* $F \subseteq G$, *entonces* $H \circ F \subseteq H \circ G$ *y* $F \circ H \subseteq G \circ H$.
5. $(F^{-1})^{-1} = F$.
6. $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$.

Demostración.

3. Sea $(x, y) \in (G \cap H) \circ F$. Entonces, existe z tal que $(x, z) \in G \cap H$ y $(z, y) \in F$. Esto implica que existe z tal que $(x, z) \in G$ y $(z, y) \in G$, vale decir, $(x, y) \in G \circ F$. Pero, además, $(x, z) \in H$ y $(z, y) \in F$, o sea, $(x, y) \in H \circ F$, o sea,

$$(G \cap H) \circ F \subseteq (G \circ F) \cap (H \circ F).$$

La otra afirmación se demuestra en forma similar.

6. Sea $(x, y) \in (G \circ F)^{-1}$. Entonces $(y, x) \in G \circ F$, o sea, existe z tal que $(y, z) \in F$ y $(z, x) \in G$. Esto equivale a decir que existe z tal que $(x, z) \in G^{-1}$ y $(z, y) \in F^{-1}$, o sea, $(x, y) \in F^{-1} \circ G^{-1}$, luego

$$(G \circ F)^{-1} \subseteq F^{-1} \circ G^{-1}.$$

La inclusión inversa se demuestra en forma análoga y se deja como ejercicio. □

Teorema 1.19. *Sean F y G funciones (o relaciones) y A y B conjuntos.*

1. $F[\emptyset] = \emptyset$.
2. $F[(A \cup B)] = F[A] \cup F[B]$.
3. $F[(A \cap B)] \subseteq F[A] \cap F[B]$.
4. $F[A] - F[B] \subseteq F[(A - B)]$.
5. *Si* $A \subseteq B$, *entonces* $F[A] \subseteq F[B]$.
6. $(G \circ F)[A] = G[(F[A])]$.
7. $F[A] \subseteq \text{Rec } F$.

Demostración.
3. Supongamos que $x \in F[(A \cap B)]$. Entonces, para algún $y \in A \cap B$, $(y, x) \in F$. Es decir, para algún $y \in A$ se verifica que $(y, x) \in F$, o sea, $x \in F[A]$. De la misma manera, para algún $y \in B$ se verifica que $(y, x) \in F$, o sea, $x \in F[B]$. Por lo tanto, $x \in F[A] \cap F[B]$, es decir, $F[(A \cap B)] \subseteq F[A] \cap F[B]$.

Para ver que la inclusión en el otro sentido no es válida, basta el siguiente contraejemplo. Sean

$$A = \{\emptyset\}\ , \quad B = \{\{\emptyset\}\} \text{ y } F = \{(\emptyset, \emptyset), (\{\emptyset\}, \emptyset)\}.$$

Entonces $A \cap B = \emptyset$, luego $F[(A \cap B)] = \emptyset$. Pero $F[A] = \{\emptyset\}$ y $F[B] = \{\emptyset\}$ luego $F[A] \cap F[B] = \{\emptyset\} \neq \emptyset$. □

Teorema 1.20. *Sean F y G funciones. Se tiene*

1. $x \in F^{-1}[a]$ *si y solo si* $F(x) \in a$.
2. F *es inyectiva si y solo si* F^{-1} *es función.*

Demostración. Demostraremos 1.

$$\begin{array}{lll} x \in F^{-1}[a] & \text{si y solo si} \quad (y, x) \in F^{-1} & \text{para algún } y \in a \\ & \text{si y solo si} \quad (x, y) \in F & \text{para algún } y \in a \\ & \text{si y solo si} \quad y = F(x) & \text{para algún } y \in a \\ & \text{si y solo si} \quad F(x) \in a. & \end{array}$$

La demostración de 2 queda como ejercicio. □

Teorema 1.21. *Sean F , G funciones. Se tiene*

1. $F^{-1}[(a \cap b)] = F^{-1}[a] \cap F^{-1}[b]$,
2. $F^{-1}[(a - b)] = F^{-1}[a] - F^{-1}[b]$.

Demostración. 1. Por el Teorema 1.19,3, basta demostrar que $F^{-1}[a] \cap F^{-1}[b] \subseteq F^{-1}[(a \cap b)]$.

Sea $x \in F^{-1}[a] \cap F^{-1}[b]$. Entonces, por Teorema 1.20,1, $F(x) \in a$ y $F(x) \in b$, o sea, $F(x) \in a \cap b$, luego $x \in F^{-1}[(a \cap b)]$.

2. Ejercicio. □

Definición 1.22.

1. Si a es un conjunto, la función
$$\begin{aligned} I_a : a &\longrightarrow a \\ x &\longmapsto x \end{aligned}$$
se llama la función *identidad* en a.
2. Si $F \in {}^a b$ es una función y C un conjunto. La *restricción de* F *a* C, $F \restriction C$, es la función
$$\begin{aligned} F \restriction C : C \cap \operatorname{Dom} F &\longrightarrow b \\ x &\longmapsto F \restriction C(x) = F(x). \end{aligned}$$

El siguiente teorema nos permite "pegar" funciones que coinciden en la parte común de sus dominios.

Teorema 1.23. *Sean* F *y* G *funciones tales que* $F \restriction a = G \restriction a$, *donde* $a = \operatorname{Dom} F \cap \operatorname{Dom} G$. *Entonces* $F \cup G$ *es una función.*

Demostración.

Recordemos que $\operatorname{Dom}(F \cup G) = \operatorname{Dom} F \cup \operatorname{Dom} G$.

Si $x \in \operatorname{Dom} F - \operatorname{Dom} G$ o $x \in \operatorname{Dom} G - \operatorname{Dom} F$, entonces es claro que existe un único y tal que $(x, y) \in F \cup G$.

Como F y G son funciones, para $x \in \operatorname{Dom} F \cap \operatorname{Dom} G$, existe un único y y un único z tal que $(x, y) \in F$ y $(x, z) \in G$. Pero, por hipótesis $y = z$, luego en este caso también hay un único y tal que $(x, y) \in F \cup G$. □

Observemos en el teorema anterior que si $\operatorname{Dom} F \cap \operatorname{Dom} G = \emptyset$, entonces $F \cup G$ es una función.

El próximo teorema es muy útil para probar que ciertas funciones son inyectivas o sobreyectivas.

Teorema 1.24. *Sea* $F : a \longrightarrow b$.

1. *Si existe una función* $G : b \longrightarrow a$ *tal que* $F \circ G = I_b$, *entonces* F *es sobreyectiva.*
2. *La función* F *es inyectiva si y solo si* $a = \emptyset$ *o bien* $a \neq \emptyset$ *y existe una función* $G : b \longrightarrow a$ *tal que* $G \circ F = I_a$.
3. F *es biyectiva si y solo si existe una función* $G : b \longrightarrow a$ *tal que* $F \circ G = I_b$ *y* $G \circ F = I_a$. *En este caso* $G = F^{-1}$.

Demostración. 1. Sea $G : b \longrightarrow a$ tal que $F \circ G = I_b$. Entonces, para todo $y \in b$, se tiene $G(y) \in a$ y
$$F(G(y)) = F \circ G(y) = I_b(y) = y\,,$$
es decir, F es sobreyectiva.

2. ($\Rightarrow$) Supongamos F es inyectiva y $a \neq \emptyset$. Sea $c \in a$ y definamos
$$G = F^{-1} \cup \{(x, c) : x \in b - F[a]\}$$

(Obsérvese que G es, efectivamente, un conjunto, ¿cómo verificamos esto?)

Es fácil ver que G es una función tal que Dom $G = b$. Para todo $x \in a$,

$$G \circ F(x) = G(F(x)) = F^{-1}(F(x)) = x,$$

ya que $F(x) \in F[a]$. Y como Dom $G \circ F =$ Dom $F = a$, $G \circ F = I_a$.

($\Leftarrow$) Si $a = \emptyset$, entonces $F = \emptyset$ y, por lo tanto, F es trivialmente inyectiva.

Si $a \neq \emptyset$ y existe $G : b \longrightarrow a$ tal que $G \circ F = I_a$. Supongamos que $F(x) = F(y)$. Entonces $G(F(x)) = G(F(y))$, o sea, $x = G \circ F(x) = G \circ F(y) = y$, luego F es inyectiva.

3. Ejercicio. □

Notemos que en el item 1 del teorema anterior, no tenemos una equivalencia como en 2 y 3. Para demostrar el recíproco de 1, es decir, si F es sobreyectiva, entonces existe $G : b \to a$ tal que $F \circ G = I_b$, necesitamos elegir para cada $y \in b$ un elemento de $F^{-1}[b]$, ese elemento es $G(y)$. Si b es un conjunto infinito habría que elegir un elemento de cada uno de infinitos conjuntos. Esto no se puede realizar tan sencillamente, para poder hacerlo se necesita un nuevo axioma, el Axioma de Elección[10]. Debido a su importancia le dedicaremos una sección completa en el Capítulo 4, sólo entonces podremos analizar este problema apropiadamente.

1.2.3 Relaciones de Orden

Una relación $R \subseteq P \times P$ es una *relación de orden parcial* sobre el conjunto P si se verifican las siguientes condiciones. (Como es habitual, escribimos $x \leq y$ en lugar de $(x, y) \in R$).

O1	Para todo $x \in P$, $x \leq x$.	Reflexividad
O2	Si $x \leq y$ e $y \leq x$, entonces $x = y$.	Antisimetría
O3	Si $x \leq y$ e $y \leq z$, entonces $x \leq z$.	Transitividad

Si además $\leq$ verifica:

O4	Para todo $x, y \in P$, $x \leq y$ ó $y \leq x$,	Conexión

decimos que el orden es *total* o *lineal*.

Si $x \leq y$ o bien $y \leq x$ los conjuntos x e y son *comparables*. Todos los elementos de un orden total son comparables entre sí. Es habitual también emplear la notación $x < y$ para denotar la relación $x \leq y$ con $x \neq y$. Siguiendo la nomenclatura habitual en matemática, si $x \leq y$ decimos que x es *menor o igual* que y o que y es *mayor o igual* que x. Análogamente, si $x < y$ decimos que x es *estrictamente menor* que y o que y es *estrictamente mayor* que x.

[10] El axioma de elección no forma parte de la teoría ZF. Sin embargo, es necesario para teoremas muy importantes de la matemática por lo que cualquier estudio de la teoría de conjuntos lo incluye. A menudo se denota ZFC a la teoría de Zermelo–Fraenkel con axioma de elección, la C es por "choice", elección en inglés.

Si existe un orden parcial definido sobre P decimos que P es un *conjunto parcialmente ordenado* por $\leq$, o simplemente, que P es un *orden parcial* sin mencionar la relación cuando ésta se subentiende. Si el orden es total, decimos que P es un *conjunto totalmente ordenado*. En estricto rigor, un conjunto parcialmente (o totalmente) ordenado es un par $(P, \leq)$, donde P es un conjunto no vacío y $\leq$ es una relación de orden parcial (o total) sobre P.

Ejemplos 1.25.

1. Los conjuntos de números $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ con su orden habitual son conjuntos totalmente ordenados.
2. Si P es un conjunto de conjuntos, por ejemplo, $P = \mathcal{P}(X)$, para algún conjunto X, entonces la relación definida entre dos elementos de P por $a \subseteq b$ es una relación de orden. Decimos que P está ordenado por *inclusión*.

   En general, éste no es un orden total, por ejemplo, si el conjunto X es el de los números naturales entonces los subconjuntos de los números pares y el de los números impares no son comparables, ¿bajo qué condiciones $\mathcal{P}(X)$ es un orden total?

   Los conjuntos ordenados por la relación $\subseteq$ los llamamos *órdenes de conjuntos*.
3. El orden $(\mathbb{N}, |\,)$ donde la relación está dada por

$$x \,|\, y \quad \text{si y solo si} \quad x \ \text{ divide a } \ y,$$

   es un orden parcial.
4. Sobre $\mathbb{Z} \times \mathbb{Z}$, el conjunto de los pares ordenados de números enteros, se define el *orden producto*

$$(a, b) \leq (c, d) \quad \text{si y solo si} \quad a \leq c \quad \text{y} \quad b \leq d.$$

   Este ejemplo se puede generalizar a cualquier número de órdenes. Si para cada $i = 1, 2 \ldots, n$, $(P_i, \leq_i)$ es un orden, entonces $(P_1 \times P_2 \times \cdots \times P_n, \leq)$, donde

$$(a_1, \ldots, a_n) \leq (b_1, \ldots b_n) \quad \text{si y solo si} \quad a_i \leq_i b_i \ \text{ para todo } \ i = 1, \ldots, n,$$

   es un orden. Observe que este es, en general, un orden parcial, ¿bajo qué condiciones es el producto de dos órdenes es un orden total?
5. El orden anterior es bastante natural para el conjunto $\mathbb{Z} \times \mathbb{Z}$. Sin embargo, existen otras maneras de ordenarlo y que también resultan "naturales". Definamos

$$(a, b) \leq_{\mathcal{L}} (c, d) \quad \text{si y solo si} \quad a < c \quad \text{o bien} \quad a = c \quad \text{y} \quad b \leq d.$$

   Denotamos este orden $(\mathbb{Z} \otimes \mathbb{Z}, \leq_{\mathcal{L}})$ y lo llamamos el *orden lexicográfico* sobre $\mathbb{Z} \times \mathbb{Z}$ porque imita el orden alfabético usado para ordenar las palabras en los diccionarios. Es claro que el orden lexicográfico puede también extenderse a productos cartesianos de cualquier número de órdenes totales. El orden lexicográfico de órdenes totales es un orden total.

6. Dado un orden $(P, \leq)$ y un conjunto cualquiera I (no necesariamente ordenado), el conjunto ${}^{I}P = \{f : I \longrightarrow P\}$ ordenado por

$$f \preceq g \quad \text{si y solo si} \quad \text{para todo } x \in P, \ f(x) \leq g(x)\,.$$

es un orden. Por ejemplo, en el conjunto de todas las funciones $f : \mathbb{R} \longrightarrow \mathbb{R}$, si tomamos $f(x) = x$ y $g(x) = x^2 + 1$, entonces $f \preceq g$, porque para todo $x \in \mathbb{R}$, $x \leq x^2 + 1$.

Para el orden definido en este ejemplo, es fácil determinar gráficamente si $f \preceq g$, en efecto, el gráfico de f debe quedar totalmente por debajo del gráfico de g.

Hemos usado el símbolo $\preceq$ para el orden de las funciones y el habitual $\leq$ para el orden en los reales con el propósito de hacer una clara distinción. Cuando, como en este caso, no hay riesgo de confusión, es habitual emplear el mismo símbolo para todos los órdenes.

7. Si $(P, \leq)$ es un orden, entonces $(P, \leq^*)$, donde

$$x \leq^* y \quad \text{si y solo si} \quad y \leq x,$$

es también un orden, llamado el orden inverso de $\leq$. (Es fácil ver que no es más que la relación inversa, en el sentido mencionado antes).

8. Dado un orden $(P, \leq)$, cualquier subconjunto $Q \subseteq P$ ordenado por la restricción del orden de P a Q es también un orden, llamado el *orden heredado*. Decimos que Q es un *suborden* de P.

Hay muchos conceptos que se usan continuamente en matemática que están relacionados con órdenes.

Definición 1.26. Un elemento del orden P se dice *minimal* si no existe ningún elemento que sea menor que él. Similarmente, un elemento es *maximal* si no hay elementos mayores que él.

Un elemento es *mínimo* si es menor o igual que todos los elementos del conjunto P. Similarmente, un elemento es *máximo* si es mayor o igual que todos los elementos del conjunto P.

Una *P–cadena*, dentro del orden P es un subconjunto totalmente ordenado. Si se subentiende cuál es el orden hablamos simplemente de una *cadena*.

Un elemento b es una *cota superior* de $A \subseteq P$ si para todo $a \in A$, $a \leq b$. Similarmente, c es una *cota inferior* de A si para todo $a \in A$, $c \leq a$.

La menor de las cotas superiores de un conjunto, si ésta existe, se llama el *supremo* del conjunto. La mayor de las cotas inferiores, si existe, es su *ínfimo*.

Ejemplos 1.27.

1. Los elementos máximos y mínimos son únicos. Lo mismo ocurre con los supremos e ínfimos.
2. Si un conjunto tiene un máximo elemento, entonces éste es una cota superior. Naturalmente tiene que ser el supremo del conjunto. Algo análogo ocurre con el mínimo.

3. Es importante no confundir elementos minimales (maximales) con el mínimo (máximo) elemento de P.

   Para un conjunto $X \neq \emptyset$, consideramos el orden $(\mathcal{P}(X) - \{\emptyset\}, \subseteq)$. Este orden no tiene mínimo, sin embargo, todo singleton $\{x\}$, con $x \in X$, es un elemento minimal. Obviamente X es el máximo.
4. Análogamente $(\mathcal{P}(X) - \{X\}, \subseteq)$ no tiene máximo, sin embargo, todo conjunto de la forma $X - \{x\}$, con $x \in X$, es un elemento maximal. Obviamente $\emptyset$ es el mínimo.
5. También es importante distinguir entre máximos y supremos, y entre mínimos e ínfimos. Por ejemplo, consideremos el subconjunto de los números reales $A = \{\frac{n-1}{n} : n \text{ es un entero positivo}\}$. Este conjunto no tiene elemento máximo, pero 1 es su supremo.
6. Si X es un conjunto infinito y $\mathcal{P}_0(X)$ es el conjunto de los subconjuntos finitos de X, entonces $(\mathcal{P}_0(X), \subseteq)$ no tiene elementos maximales. En este caso $\emptyset$ es el único elemento minimal y por ende es el menor elemento.

Definición 1.28. Una función $\varphi : P_1 \longrightarrow P_2$ de un orden $(P_1, \leq_1)$ en un orden $(P_2, \leq_2)$ se dice *isótona* (o *creciente*) si se verifica:

$$x \leq_1 y \;\Rightarrow\; \varphi(x) \leq_2 \varphi(y).$$

Una función biyectiva $\varphi : P_1 \longrightarrow P_2$ de un orden $(P_1, \leq_1)$ en $(P_2, \leq_2)$ es un *isomorfismo de orden* si se verifica:

$$x \leq_1 y \quad \text{si y solo si} \quad \varphi(x) \leq_2 \varphi(y).$$

En este caso decimos también que los órdenes P_1 y P_2 son *isomorfos*.

Obsérvese que por tratarse de una biyección (luego inyectiva), la definición de isomorfismo implica que

$$x <_1 y \quad \text{si y solo si} \quad \varphi(x) <_2 \varphi(y).$$

También es inmediato de la definición que si φ es un isomorfismo de orden, entonces $\varphi^{-1} : P_2 \longrightarrow P_1$ también lo es.

Ejemplo 1.29. El conjunto P de los enteros positivos pares con el orden heredado es isomorfo con $\mathbb{N}$. Basta definir

$$\begin{aligned} \varphi : \mathbb{N} &\longrightarrow P \\ n &\longmapsto 2n \end{aligned}$$

y comprobar que esta es una biyección isótona tal que su inversa también es isótona.

No es tan directo demostrar que no existe un isomorfismo entre $\mathbb{N}$ y $\mathbb{Z}$. Para verlo, supongamos que sí existe. Entonces consideramos $\varphi(0) - 1 \in \mathbb{Z}$. Como φ es en particular sobreyectiva, debe existir un entero positivo n tan que $\varphi(n) = \varphi(0) - 1$. Entonces $\varphi(n) < \varphi(0)$ y por la definición de isomorfismo, se tiene $n < 0$, lo que es una contradicción. Por lo tanto, no puede existir tal isomorfismo.

Este ejemplo ilustra el significado de que dos órdenes sean isomorfos: ambos deben tener las mismas propiedades de orden. En nuestro ejemplo, $\mathbb{N}$ tiene un menor elemento y $\mathbb{Z}$ no lo tiene, luego no pueden ser isomorfos. Por supuesto, esta es una afirmación extremadamente vaga ya que no hemos dicho qué es una "propiedad"de orden. El siguiente teorema nos da una idea de lo que queremos decir y resulta muy útil para demostrar que dos órdenes NO son isomorfos. Su demostración se deja como ejercicio.

Teorema 1.30. *Un isomorfismo de orden preserva mínimo, máximo, elementos minimales y maximales. Más precisamente, si* φ *es un isomorfismo y* a *es mínimo, máximo, minimal o maximal, entonces también lo es* $\varphi(a)$*.*

Es interesante observar que una biyección isótona no tiene por qué ser un isomorfismo de orden, como lo demuestra la función $F : \{a, b, c, d\} \longrightarrow \{0, 1, 2, 3\}$ indicada en el diagrama siguiente. En éste, el orden queda representado por la posición relativa de los puntos, así, $x < y$ si hay un camino ascendente desde x hasta y. Basta observar que la inversa F^{-1} no es isótona, en efecto, $1 < 2$, sin embargo, $b \not< c$.

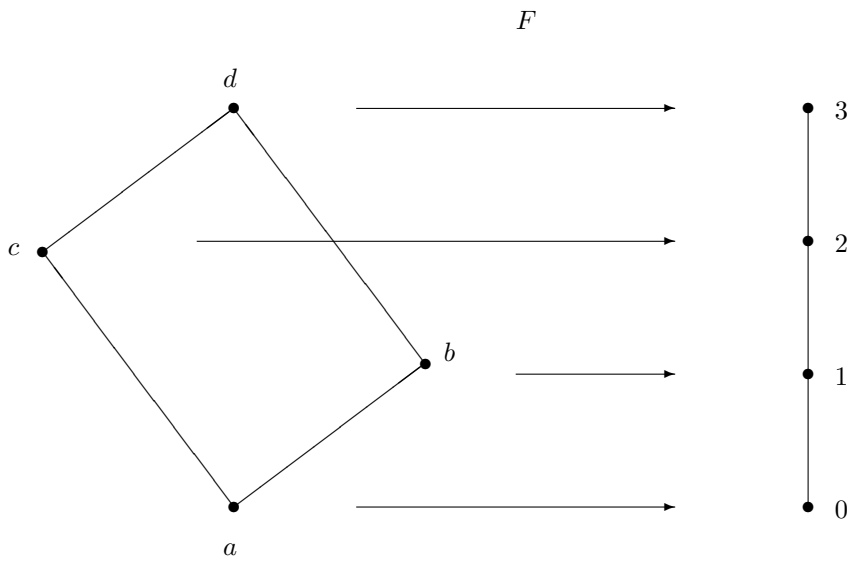


Diagrama 1. Una biyección isótona que no es un isomorfismo de orden.

Un ejemplo importante de órdenes isomorfos es el siguiente. Dado un conjunto X, consideremos el conjunto ${}^{X}\{0, 1\}$ de todas las funciones de X en $\{0, 1\}$ ordenado según el orden definido en el ejemplo 6 de los ejemplos 1.25. El orden del conjunto $\{0, 1\}$ está dado por $0 < 1$.

Teorema 1.31.
Sea X un conjunto. Entonces $(\mathcal{P}(X), \subseteq)$ es isomorfo con $({}^{X}\{0,1\}, \leq)$.

Demostración. Dado $A \in \mathcal{P}(X)$ definimos su *función característica* como sigue:

$$\chi_A : X \longrightarrow \mathbf{D},$$
$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

Entonces

$$\begin{aligned} \varphi : \mathcal{P}(X) &\longrightarrow {}^{X}\mathbf{D} \\ A &\longmapsto \chi_A \end{aligned}$$

es un isomorfismo de orden.

Para ver que φ es inyectiva debemos verificar que si $\chi_A = \chi_B$, entonces $A = B$. Supongamos que $\chi_A = \chi_B$. Si $x \in A$, entonces $\chi_A(x) = 1$, luego $\chi_B(x) = 1$, o sea $x \in B$, vale decir $A \subseteq B$. De igual forma se prueba que $B \subseteq A$, por lo tanto, $A = B$.

Para ver que φ es sobreyectiva debemos verificar que si $f \in {}^{X}\mathbf{D}$, entonces para algún $A \subseteq X$, $f = \varphi(A)$. Recordemos que f es una función cuyo recorrido está contenido en $\mathbf{D} = \{0,1\}$. Definimos

$$A = f^{-1}[\{1\}] = \{x \in X \,:\, f(x) = 1)\} \subseteq X\,.$$

Entonces

$$f(x) = 1 \text{ si y solo si } x \in A \text{ si y solo si } \chi_A(x) = 1\,,$$

o sea, las funciones f y χ_A son iguales y $f = \varphi(A)$.

Por último para ver que φ es isomorfismo de orden vemos

$$A \subseteq B \quad \text{si y solo si} \quad \chi_A \leq \chi_B\,.$$

Si $A \subseteq B$ y $\chi_A(x) = 1$, entonces $x \in A$, luego $x \in B$, y entonces $\chi_B(x) = 1$, por lo tanto, $\chi_A(x) \leq \chi_B(x)$. Por otra parte, es claro que si $\chi_A(x) = 0$, entonces también $\chi_A(x) \leq \chi_B(x)$. Luego, en cualquier caso, para todo $x \in X$, $\chi_A(x) \leq \chi_B(x)$, o sea, por definición, $\chi_A \leq \chi_B$.

Recíprocamente, si $\chi_A \leq \chi_B$ y $x \in A$, $\chi_A(x) = 1$, luego $\chi_B(x) = 1$, o sea $x \in B$, vale decir $A \subseteq B$. Esto completa la demostración de que φ es un isomorfismo de orden. □

Teorema 1.32. *Todo orden es isomorfo con un orden de conjuntos.*

Demostración. Sea $(P, \leq)$ un orden. Para cada $a \in P$, definimos el conjunto $\mathcal{I}(a) = \{x : x \leq a\}$. Entonces $Q = \{\mathcal{I}(a) : a \in P\}$, ordenado por inclusión es un suborden de conjuntos de $\mathcal{P}(P)$ isomorfo con $(P, \leq)$, (ver Ejemplo 2 de 1.25). En efecto, definimos

$$\begin{aligned} \mathcal{I} : P &\longrightarrow Q \\ a &\longmapsto \mathcal{I}(a) \end{aligned}$$

Entonces, si $a \leq b$, y $x \in \mathcal{I}(a)$, $x \leq b$ y, por lo tanto, $\mathcal{I}(a) \subseteq \mathcal{I}(b)$.

Recíprocamente, si $\mathcal{I}(a) \subseteq \mathcal{I}(b)$, como $a \in \mathcal{I}(a)$, $a \in \mathcal{I}(b)$ y, por lo tanto, $a \leq b$.

Por otra parte, debido a la antisimetría, $\mathcal{I}$ es inyectiva. La sobreyectividad es inmediata de la definición de Q. □

1.2.3 Buenos Órdenes

Terminamos esta subsección con un concepto que tiene mucha importancia, desde la teoría elemental de números hasta temas muy avanzados de matemática.

Decimos que $(P, \leq)$ es un *buen orden* (o que P está *bien ordenado*) si todo subconjunto no vacío de P contiene un elemento mínimo.

El ejemplo clásico de buen orden es el conjunto $\mathbb{N}$ de los enteros positivos. Por su parte, $\mathbb{Z}$ con su orden habitual no está bien ordenado, así como tampoco el intervalo $[0, 1]$ de los números reales con el orden heredado. En el primer caso el subconjunto $\mathbb{Z}$ mismo no tiene menor elemento, en el segundo, el intervalo semi–abierto (y obviamente no vacío) $(\frac{1}{2}, 1]$ no tiene un menor elemento. Un error habitual es confundir el menor elemento con el ínfimo. En el último ejemplo se puede pensar que $\frac{1}{2}$ es el menor elemento de $(\frac{1}{2}, 1]$, sin embargo, no lo es, porque $\frac{1}{2} \notin (\frac{1}{2}, 1]$.

Observación 1.3. Es fácil ver que un conjunto bien ordenado es totalmente ordenado. En efecto, dados dos elementos x e y del conjunto bien ordenado P, podemos considerar el subconjunto no vacío $\{x, y\}$ de P. Éste debe tener un menor elemento, digamos x. Entonces $x \leq y$, por lo tanto, todos los elementos de P son comparables entre sí.

El siguiente teorema es un resultado sorprendente.

Teorema 1.33. Teorema de Zermelo.
Todo conjunto puede bien ordenarse.

Si uno piensa, por ejemplo, en los números reales, es difícil imaginarse como podrían reordenarse para que siempre podamos encontrar el más pequeño de cada subconjunto. Para tratar de imaginarnos cómo debe ser tal orden debemos primero sacar de nuestra cabeza el orden habitual, ese no sirve. Pensamos primero en el conjunto $\mathbb{R}$ y tomamos un elemento al azar, digamos π. Éste es nuestro primer elemento en el nuevo orden, ahora consideramos el subconjunto no vacío $\mathbb{R} - \{\pi\}$, y escogemos otro al azar, digamos $-\sqrt{3}$ y decimos que éste es el que sigue, es decir, $\pi \prec -\sqrt{3}$. Ahora miramos el subconjunto no vacío $\mathbb{R} - \{\pi, -\sqrt{3}\}$, y escogemos otro al azar... Podemos seguir con este procedimiento y vamos a cada paso bien ordenando los números reales. Pero hay un problema. Como veremos en el Capítulo 3, este procedimiento nunca cubrirá a todos los números reales.

1.2.4 Relaciones de Equivalencia

Una *relación de equivalencia* sobre un conjunto A es una relación $\sim$ tal que para todo $a, b, c \in A$ se satisface:

(E1) $a \sim a$. Reflexividad
(E2) Si $a \sim b$, entonces $b \sim a$. Simetría
(E3) Si $a \sim b$ y $b \sim c$, entonces $a \sim c$. Transitividad

Ejemplos 1.34.

1. El primer ejemplo de relación de equivalencia es el más trivial: la igualdad. La reflexividad, a menudo conocida como el principio de identidad, nos dice que todas las cosas son iguales a sí mismas; la simetría nos dice que si una cosa es igual a otra, entonces ésta es igual a la primera; la transitividad nos dice que si una cosa es igual a otra y ésta es igual a una tercera, entonces la primera es igual a la tercera. Estas son las propiedades básicas de la identidad que se busca abstraer con el concepto de relación de equivalencia.
2. La relación de paralelismo sobre el conjunto de todas las rectas del plano es una relación de equivalencia.
3. Sobre el conjunto $\mathbb{Z}$ de los números enteros definimos la relación

$$a \sim_n b \qquad \text{si y solo si} \qquad n \mid (b - a)\,,$$

donde $x \mid y$ significa que x divide a y. Esta es una relación de equivalencia llamada congruencia módulo n. Esta relación es extremadamente importante en teoría de números. Más información puede encontrarse, por ejemplo, en [**7**].
4. La idea de relación de equivalencia se puede extender a cualquier ámbito del pensamiento y no sólo dentro de la matemática. Por ejemplo, sobre el conjunto de los seres humanos podemos establecer la relación "tener la misma edad". Ésta es una relación de equivalencia. Reflexividad, simetría y transitividad se obtienen aquí de las correspondientes propiedades de la identidad.

   Más generalmente, cualquier relación definida sobre un conjunto mediante la expresión "tener el mismo $\mathcal{P}$", donde $\mathcal{P}$ es una propiedad adecuada de los objetos del conjunto, será una relación de equivalencia. No desarrollaremos esta idea en este libro.
5. Siempre existen dos relaciones de equivalencia sobre un conjunto $A \neq \emptyset$, a saber, la identidad y la relación completa, es decir, $A \times A$, ¿qué sucede si $A = \emptyset$?

Reflexividad, simetría y transitividad son en un sentido particular las propiedades esenciales de la identidad. Una relación con esas propiedades nos permite identificar objetos que comparten ciertas características, de modo que uno puede tratarlos como un solo objeto. Resulta útil entonces dar un nombre a los conjuntos de elementos relacionados entre sí. Los llamaremos *clases de equivalencia*. Más técnicamente, la *clase de equivalencia de* a *módulo* $\sim$ es el conjunto[11]:

$$[a]_\sim = \{x \in A : x \sim a\}\,.$$

El conjunto $A\,|_\sim$ de todas las clases de equivalencia se llama *cuociente de* A *módulo* $\sim$.

Obsérvese que los conjunto $[a]_\sim$ y $A \mid \sim$ están bien definidos por el Axioma de Separación.

Ejemplos 1.35.

1. Si la relación de equivalencia es paralelismo entre las rectas del plano, entonces cada clase de equivalencia está constituida por todas las rectas que son paralelas entre sí. Por ejemplo, la clase de equivalencia del eje X es el conjunto de todas las rectas horizontales. Hay tantas clases de equivalencia como pendientes posibles más la clase de todas las rectas verticales.
2. Si la relación de equivalencia es congruencia módulo 2 sobre los números enteros, entonces hay dos clases de equivalencia, el conjunto de los números pares y el de los impares.

Teorema 1.36. *Para todo* $a\,,\, b \in A$

$$a \sim b \quad \textit{si y solo si} \quad [a]_\sim = [b]_\sim\,.$$

Demostración. Supongamos que $a \sim b$ y que $x \in [a]_\sim$. Entonces, $x \sim a$ y como $a \sim b$, por transitividad, $x \sim b$. Pero, entonces $x \in [b]_\sim$ y, por lo tanto, $[a]_\sim \subseteq [b]_\sim$. La inclusión en el otro sentido es análoga.

Supongamos ahora que $[a]_\sim = [b]_\sim$. Entonces, como por reflexividad $a \in [a]_\sim$, también $a \in [b]_\sim$ y por definición $a \sim b$. □

Una *partición* de un conjunto X es un conjunto P de subconjuntos de X tal que

(P1) $A \neq \emptyset$, para cada $A \in P$.
(P2) $A \cap B = \emptyset$, para $A \neq B$.
(P3) $X = \bigcup P$.

[11] La notación más estándar para la clase de equivalencia de a es $\overline{a}$. En este texto no la usaremos porque, en presencia de varias relaciones de equivalencia sobre un mismo conjunto, no distingue con respecto a cuál de ellas se está tomando la clase. Esto podría resultar particularmente confuso, por ejemplo, en el Capítulo 2. Por otra parte, la barra superior tiene muchos otros usos en matemática.

Intuitivamente, una partición cubre al conjunto X en partes no vacías y disjuntas. Los elementos de una partición se llaman *bloques*.

Teorema 1.37. *Si P es una partición de X entonces la relación*

$$a \sim_P b \qquad \text{si y solo si para algún } A \in P\,,\ a, b \in A$$

es una relación de equivalencia.

Las clases de equivalencia módulo $\sim_P$ son los bloques de P.

Demostración. Como vemos, esta relación se establece entre los elementos que pertenecen al mismo bloque de la partición. Por (P3) todo $a \in X$, pertenece a algún bloque A. Obviamente a pertenece al mismo bloque que él mismo, luego, $a \sim_P a$, o sea, la relación es reflexiva.

Si a y b están en el mismo bloque, entonces también b y a lo están, es decir, la relación es simétrica.

Si $a \sim_P b$ y $b \sim_P c$, entonces $a, b \in A$, y $b, c \in B$, para ciertos bloques A, y $B \in P$. Pero entonces, $b \in A \cap B$ y por (P2), esto sólo puede ser cierto si $A = B$, luego tanto a como c pertenecen al mismo bloque, o sea, $a \sim_P c$ y la relación es transitiva.

Es claro que los bloques de P son las clases de equivalencia. □

Recíprocamente, es fácil ver que el conjunto $A\,|\sim$ de todas estas clases de equivalencia es una partición de A.

Teorema 1.38. *Si $\sim$ es una relación de equivalencia sobre A entonces el conjunto $A \mid \sim = \{[a]_\sim : a \in A\}$ de las clases de equivalencia módulo $\sim$, es una partición de A.*

Para facilitar la lectura, hemos descrito $A \mid \sim$ de manera informal, sin embargo, es fácil ver que se trata efectivamente de un conjunto. En efecto,

$$A \mid \sim = \{x \in \mathcal{P}(A) : x = [a]_\sim\,,\ \text{ para algún } a \in A\}$$

es un conjunto en virtud del Axioma de Separación.

Demostración. Dada una clase $[a]_\sim$, entonces $a \in [a]_\sim$, o sea $[a]_\sim \neq \emptyset$, y se verifica (P1).

Supongamos que $[a]_\sim$ y $[b]_\sim$ son clases distintas. Entonces, si $c \in [a]_\sim \cap [b]_\sim$, $c \sim a$ y $c \sim b$, luego por transitividad, $a \sim b$. Pero, entonces $[a]_\sim = [b]_\sim$, lo que contradice nuestra elección de las clases. Esto demuestra (P2).

Como todo elemento pertenece a su clase de equivalencia, es también claro que $A = \bigcup\{[a]_\sim : a \in A\}$, por lo que también (P3) es válido y $A \mid \sim$ es una partición de A. □

Teorema 1.39.

1. *Sean* $\sim$ *una relación de equivalencia y* $A \mid_{\sim}$ *la partición definida por sus clases de equivalencia. Entonces la relación de equivalencia* $\sim_{A|_{\sim}}$ *asociada a esta partición es igual a* $\sim$.
2. *Sean* P *una partición de* A *y* $\sim_P$ *su relación de equivalencia asociada. Entonces la partición* $A \mid_{\sim_P}$ *asociada a esta relación de equivalencia es igual a* P.

Demostración.

1. $a \sim_{A|_{\sim}} b$ si y solamente si a y b pertenecen al mismo bloque de la partición $A_{\sim}$, esto es si y solamente si a y b pertenecen a la misma clase de equivalencia módulo $\sim$ y esto es si y solamente si $a \sim b$.

2. Un bloque B pertenece a la partición $A \mid_{\sim}$ si y solamente si B es una clase de equivalencia módulo $\sim_P$ y esto es si y solamente si B es un bloque de la partición P. □

Veremos para finalizar esta sección un caso muy natural y de frecuente ocurrencia de partición y, por ende, de relación de equivalencia sobre un conjunto.

Teorema 1.40. *Sea* $f : A \longrightarrow B$ *una función. Entonces*

1. *La relación definida por* $a \sim b$ *si y solo si* $f(a) = f(b)$ *es una relación de equivalencia.*
2. *El conjunto* $P = \{f^{-1}[b] : b \in \mathrm{Rec} f\}$ *es una partición de* A.
3. *Esta relación y partición están asociadas de la manera descrita en los teoremas anteriores, es decir,* $P = A \mid_{\sim}$.

Demostración.

1. Esto es consecuencia directa de las correspondientes propiedades de la identidad.

2. Si $b \in \mathrm{Rec} f$, entonces existe $a \in A$ tal que $f(a) = b$, o sea, $f^{-1}[b] \neq \emptyset$.
   Supongamos que $b \neq b'$. Si $x \in f^{-1}(b) \cap f^{-1}(b')$, entonces $b = f(x) = b'$, una contradicción, luego $f^{-1}(b) \cap f^{-1}(b') = \emptyset$.
   Es claro que $a \in f^{-1}(f(a))$, por lo que $A = \bigcup_{b \in \mathrm{Rec} f} f^{-1}(b)$.
   Como se cumplen (P1), (P2) y (P3), P es una partición de A.

3. Esto es inmediato y se deja como ejercicio. □

1.2.5 Ejercicios

1. La definición de par ordenado que hemos dado es la más difundida en la actualidad y fue propuesta por K. Kuratowski en 1921. Sin embargo, no es la única posible. En 1914 Norbert Wiener definió

$$(x, y)_1 = \{\{\{a\}, \emptyset\}, b\}.$$

   Demuestre que si $(a, b)_1 = (c, d)_1$, entonces $a = c$ y $b = d$.

2. Existe todavía otra manera de definir pares ordenados. Definimos
$$(a,b)_2 = \{\{a,\emptyset\},\{b,\{\emptyset\}\}\}\,.$$
Demuestre que entonces se satisface:
$$(a,b)_2 = (c,d)_2 \text{ si y solo si } a=c \text{ y } b=d\,.$$
3. Proponga una manera alternativa de definir par ordenado usando las propiedades elementales de los conjuntos.
4. Sean a, b, c conjuntos. Definimos el conjunto
$$(a,b,c)' = \{\{a\},\{a,b\},\{a,b,c\}\}\,.$$
Pruebe que $(a,b,c)' = (d,e,f)'$ no implica que $a=d$ y $b=e$ y $c=f$.
5. Pruebe que:
   a) $\bigcap(a,b) = \{a\}$.
   b) $\bigcap\bigcap(a,b) = a = \bigcup\bigcap(a,b)$.
   c) $\bigcap\bigcup(a,b) = a\cap b$.
   d) $(\bigcap\bigcup(a,b)) \cup (\bigcup\bigcup(a,b) - \bigcup\bigcap(a,b)) = b$.
6. a) Pruebe que $A\times B = B\times A$ si y solo si $A=\emptyset$ ó $B=\emptyset$ ó $A=B$.
   b) Pruebe que si $A\neq\emptyset$ y $A\times B\subseteq A\times C$, entonces $B\subseteq C$.
   c) Pruebe que no es cierto : $A\times(B\times C) = (A\times B)\times C$.
   d) Pruebe que $A\times B\cap C\times D = A\times D\cap C\times D$.
   e) Pruebe que $A\times B - C\times C = (A-C)\times B\cup A\times(B-C)$
   f) Pruebe que $A\times A - B\times C = (A-B)\times A\cup A\times(A-C)$.
7. a) Encontrar todas las relaciones cuyo dominio está contenido en $\{a,b,c\}$ y cuyo recorrido está contenido en $\{s,t\}$.
   b) ¿Cuántas relaciones se pueden formar en un conjunto de n elementos?
8. Demuestre todas las afirmaciones que no se demostraron en el Teorema 1.8.
9. Demuestre todas las afirmaciones que no se demostraron en el Teorema 1.18.
10. Demuestre todas las afirmaciones que no se demostraron en el Teorema 1.12.
11. Demuestre todas las afirmaciones que no se demostraron en el Teorema 1.19.
12. Considere funciones $F:\mathbb{N}\longrightarrow\mathbb{N}$. Dé ejemplos de funciones tales que:
   a) F no es inyectiva ni sobreyectiva.
   b) F es inyectiva pero no sobreyectiva.
   c) F es sobreyectiva pero no inyectiva.
   d) F es biyectiva pero no es la identidad.
13. Pruebe que no toda inyección de un conjunto en sí mismo es sobreyectiva.
14. Sean $F: a\longrightarrow b$ y $G: a\longrightarrow b$ funciones. Pruebe que si $F\subseteq G$, entonces $F=G$.
15. Sean $F: a\longrightarrow b$ y $G: c\longrightarrow d$ funciones. Se define un producto entre F y G por
$$(F*G)(x,y) = (F(x),G(y))$$
para $(x,y)\in a\times c$. Pruebe que:
   a) $F*G$ es una función de $a\times c$ en $b\times d$.

b) Si F y G son sobreyectivas, entonces $F * G$ es sobreyectiva.
c) Si F y G son inyectivas, entonces $F * G$ es inyectiva .
d) $\text{Rec}\,(F * G) = (\text{Rec}\,F) \times (\text{Rec}\,G)$.

16. Sea $F : a \longrightarrow b$ función. Se define G por $G(y) = F^{-1}[\,\{y\}]$. Probar que G es función. Determine su dominio y su recorrido. Demuestre que si F es sobreyectiva, entonces G es inyectiva . Probar también que el recíproco es falso.
17. Determine cuáles de las siguientes relaciones son funciones:
    a) R es relación de $\mathbb{R}$ en $\mathbb{R}$ tal que $(a, b) \in R$ si y solo si $a^2 + b^2 = 1$.
    b) R es relación de $\mathbb{R}$ en $\mathbb{R}$ tal que $(a, b) \in R$ si y solo si $0 \leq a < 1$ y $b = \frac{a}{1-a}$.
    c) R es relación entre $\mathbb{R} \times \mathbb{R}$ y $\mathbb{R}$ tal que $((a, b), c) \in R$ si y solo si $c = \frac{a+b}{2}$.
18. Demuestre que si F y G son funciones inyectivas, entonces $G \circ F$ es inyectiva y $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$.
19. Construya los conjuntos ${}^{\{a,b,c\}}\{1, 2\}$, ${}^{\{1,2\}}\{a, b, c\}$.
20. Sean a, b, c conjuntos tales que $b \cap c = \emptyset$. Pruebe que existe una biyección entre ${}^{b\cup c}a$ y ${}^{b}a \times {}^{c} a$.
21. ¿Existe una biyección entre ${}^{c}({}^{b}a)$ y ${}^{b\times c}a$?
22. Pruebe que existe una biyección entre ${}^{c}(a \times b)$ y ${}^{c}a \times {}^{c} b$.
23. Sean $F : a \longrightarrow b$ y $G : c \longrightarrow d$ funciones biyectivas, donde $a \cap c = \emptyset$ y $b \cap d = \emptyset$. Sea $H = F \cup G$. Pruebe que H es biyección entre $a \cup c$ y $b \cup d$.
24. Sea $F : a \longrightarrow b$ función. Sean $c \subseteq a$ y $d \subseteq b$.
    a) Si F es inyectiva, Pruebe que $c = F^{-1}[\,F[c]\,]$.
    b) Si F es sobreyectiva, Pruebe que $d = F[F^{-1}[d]\,]$.
25. Dé un ejemplo de una función F y un conjunto a tales que $F \cap (a \times a) \neq F \restriction a$.
26. Si F y G son funciones inyectivas con el mismo dominio, probar o dar contra-ejemplo de:
    a) $F \cup G$ es inyectiva.
    b) $F - G$ es inyectiva.
    c) $a \cap b = \emptyset$ implica que $F \restriction a \cup G \restriction b$ es inyectiva.
    d) $a \cap b = \emptyset$ implica que $F[\,a] \cap G[\,b] = \emptyset$.
27. Demuestre todas las afirmaciones que no se demostraron en los Teoremas 1.17, 1.20, 1.21 y 1.24.
28. Pruebe que si R, S, T son relaciones y a, b, c conjuntos, entonces:
    a) $S \cap T$ y $S \cup T$ son relaciones .
    b) $(S \cap T)^{-1} = S^{-1} \cap T^{-1}$.
    c) $(S \cup T)^{-1} = S^{-1} \cup T^{-1}$.
    d) $(R - S)^{-1} = R^{-1} - S^{-1}$.
    e) $(R \circ S) - (R \circ T) \subseteq R \circ (S - T)$.
    f) $R \subseteq S$ si y solo si $S^{-1} \subseteq R^{-1}$.
    g) $(a \times b)^{-1} = b \times a$.
    h) Si a y b no son disjuntos, entonces $(a \times b) \circ (a \times b) \subseteq (a \times b)$.
    i) Si a y b son disjuntos, entonces $(a \times b) \circ (a \times b) = \emptyset$.

j) Si b no es vacío, entonces $(b \times c) \circ (a \times b) = a \times c$.
k) Si $R \subseteq a \times b$ y $S \subseteq b \times c$, entonces $S \circ R \subseteq a \times c$.

29. Encuente contraejemplos para las siguientes afirmaciones:
a) $\mathrm{Dom}\,(R \cap S) = \mathrm{Dom}\,R \cap \mathrm{Dom}\,S$.
b) $\mathrm{Rec}\,(R \cap S) = \mathrm{Rec}\,R \cap \mathrm{Rec}\,S$.
c) $\mathrm{Dom}\,R - \mathrm{Dom}\,S = \mathrm{Dom}\,(R - S)$.
d) $\mathrm{Rec}\,R - \mathrm{Rec}\,S = \mathrm{Rec}\,(R - S)$.
e) $R[\,(a \cap b)] = R[\,a] \cap R[\,b]$.
f) $R[\,a] - R[\,b] = R[\,(a - b)]$.
g) $R[\,a] = \mathrm{Rec}\,R$.
h) $R^{-1}[\,(\,R[a\,])] = a$.
i) $R[(\,R^{-1}\,[\,b]\,)] = b$.

30. ¿Cuántos órdenes parciales existen sobre $\{a, b\}$?, ¿sobre $\{a, b, c\}$?, ¿sobre $\{a, b, c, d\}$? Haga los diagramas correspondientes.
31. Diga cuáles de los órdenes del ejercicio anterior son isomorfos.
32. Proporcione los detalles de la definición del orden lexicográfico de los órdenes totales $(A_1, \leq_1)$, ..., $(A_n, \leq_n)$.
33. Demuestre que si P_1 y P_2 son órdenes con al menos dos elementos cada uno, entonces $P_1 \times P_2$ no es un orden total, ¿por qué es necesario exigir que haya al menos dos elementos?
34. Sean $(P_1, \leq_1)$ y $(P_1, \leq_1)$ órdenes y $P_1 \cap P_2 = \emptyset$. Definimos sobre $P_1 \cup P_2$ la relación:

$$x \preceq y \text{ si y solo si } \begin{cases} x\,,\, y \in P_1 \text{ y } x \leq_1 y, \\ x\,,\, y \in P_2 \text{ y } x \leq_2 y, \\ x \in P_1 \text{ e } y \in P_2. \end{cases}$$

Demuestre que $(P_1 \cup P_2, \preceq)$ es un orden. Demuestre que si P_1 P_2 son órdenes totales, también lo es $(P_1 \cup P_2, \preceq)$. Lo mismo si ambos son buenos órdenes.

35. Haga la construcción anterior para P_1 el conjunto de los números naturales pares y P_2 el conjunto de los números naturales impares, ambos con su orden estándar. Observe que tanto P_1 como P_2 son órdenes isomorfos a los números naturales.
36. Demuestre que si P_1 y P_2 son órdenes totales, $P_1 \otimes P_2$, el orden lexicográfico, también lo es.
37. Encuentre todas las relaciones de equivalencia sobre $\{1, 2, 3\}$. Sobre $\{1, 2, 3, 4\}$.
38. Sea R una relación. Demuestre
a) R es simétrica si y solo si $R^{-1} \subseteq R$.
b) R es transitiva si y solo si $R \circ R \subseteq R$.
c) R es simétrica y transitiva si y solo si $R^{-1} \circ R = R$.
39. Suponga que $f : A \longrightarrow B$ es una función y R una relación de equivalencia en B. Demuestre que

$$Q = \{(x, y) \in A \times A \,:\, (f(x), f(y)) \in R\}$$

es una relación de equivalencia en A.

40. Sobre el plano $\mathbb{R} \times \mathbb{R}$ consideramos todos los conjuntos $B_r = \{(x, y) : y = 2x + r\}$ donde $r \in \mathbb{R}$. Demuestre que esta es una partición, ¿cuál es la relación de equivalencia asociada?

Capítulo 2: Sistemas Numéricos

En este capítulo construiremos los conjuntos de números naturales, enteros, racionales y reales, dentro de la teoría de conjuntos. Como veremos, en esta construcción cada número será un conjunto y, a medida que avanzamos, estos conjuntos serán más y más complejos. Si bien llamaremos "números" a los objetos de los que hablaremos y los denotaremos 1, 2, 3, $\frac{2}{3}$, $\sqrt{5}$, etc., estos son en realidad conjuntos abstractos. Así mismo, las relaciones y funciones entre ellos tendrán las propiedades intuitivas que conocemos de los números y de sus operaciones. De esta manera, el conjunto que define, por ejemplo, al número entero 25, no es *el* número 25, sino sólo una suerte de representante de éste dentro del modelo formal. Acerca de la naturaleza de los números no nos pronunciaremos aquí, ya que se trata de un problema que compete más a la filosofía que a la matemática. En todo momento se debe tener presente la diferencia entre el objeto y su representante dentro del modelo.

Una segunda observación metodológica es que, precisamente porque estamos construyendo un modelo de los números que tiene todas las propiedades intuitivas de éstos, a menudo nos sentimos inclinados a atribuirles estas propiedades sin antes demostrarlas en el marco de los axiomas de la teoría de conjuntos. Nuestro trabajo es precisamente lo contrario, debemos demostrar que estos constructos teóricos efectivamente tienen las propiedades intuitivas de los números.

Por último, el lector que haya tomado un curso de álgebra abstracta, notará que muchas de las demostraciones sobre las propiedades de los números, son un caso particular de las correspondientes propiedades demostradas para grupos, anillos o cuerpos. De esta manera, las demostraciones presentadas en el texto pueden parecer repetidas y tediosas. Hemos adoptado la posición de no suponer que el lector tiene estos conocimientos de álgebra abstracta y de guiarlo a lo largo de varias demostraciones muy similares, con el propósito de verlas varias veces en contextos levemente diferentes y las incorpore así a sus conocimientos. Por otra parte, aquellos que ya han hecho estos cálculos anteriormente, simplemente pueden obviarlos.

2.1 Los Números Naturales

Formalizaremos ahora el concepto intuitivo de número natural dentro de la teoría de conjuntos.

Definición 2.1. El *sucesor* de un conjunto x es el conjunto

$$Sx = x \cup \{x\}.$$

Observe que para cualquier conjunto x su sucesor Sx también es un conjunto (¿por qué?). Obsérvese también que este "sucesor del conjunto x" está definido para cualquier conjunto y no sugiere, en principio, la idea intuitiva de que "el sucesor de x es aquel que sigue a x" en algún orden.

Es también inmediato que

$$x \subseteq Sx \quad \text{y también} \quad x \in Sx\,.$$

Esto tendrá importancia luego.

No cualquier conjunto es el sucesor de otro. Obviamente $\emptyset$ no es un sucesor, pero hay otros, por ejemplo, $\{\{\emptyset\}\}$ no es un sucesor. Si lo fuera, existiría x tal que $x \cup \{x\} = \{\{\emptyset\}\}$ y luego $x \in \{\{\emptyset\}\}$, o sea, $x = \{\emptyset\}$. Pero esto nos dice que $\emptyset \in x \subseteq \{\{\emptyset\}\}$, o sea, $\emptyset = \{\emptyset\}$, lo que es una contradicción, ya que $\{\emptyset\}$ tiene un elemento y $\emptyset$ ninguno.

2.1.1 Conjuntos inductivos

Definición 2.2. Decimos que un conjunto X es *inductivo* si

i) $\emptyset \in X$.
ii) Si $x \in X$, entonces $Sx \in X$.

El Axioma de Infinito, que será presentado en la página 121 del Capítulo 4, nos dice precisamente que existe al menos un conjunto inductivo. Tomemos un conjunto inductivo cualquiera y llamémoslo I.

Definición 2.3. El conjunto $\mathbb{N}$ de los *números naturales*[1] se define como sigue:

$$\mathbb{N} = \bigcap \{x \in \mathcal{P}(I) : \ x \quad \text{es inductivo}\}\,.$$

Los elementos de $\mathbb{N}$ se llaman *números naturales*.

El siguiente teorema nos dice que $\mathbb{N}$ es el más pequeño de los conjuntos inductivos, independientemente de cuál sea el conjunto inductivo I con el que fue definido.

Teorema 2.4. *El conjunto $\mathbb{N}$ es inductivo y si X es inductivo, entonces $\mathbb{N} \subseteq X$.*

Demostración. Como $\emptyset$ pertenece a cualquier conjunto inductivo, $\emptyset$ está en cualquier intersección de conjuntos inductivos, en particular en $\mathbb{N}$.

Sea $y \in \mathbb{N}$. Entonces, dado cualquier conjunto inductivo $J \subseteq I$, $y \in J$ y como J es inductivo, $Sy \in J$. Esto demuestra que $Sy \in \mathbb{N}$, probando que $\mathbb{N}$ es inductivo.

Si X es inductivo, entonces basta notar que $X \cap I \in \mathcal{P}(I)$ también lo es, luego por definición $\mathbb{N} \subseteq X \cap I \subseteq X$. □

[1] Los libros más técnicos de teoría de conjuntos habitualmente denotan al conjunto de los números naturales con la letra griega ω.

2.1.2 Algunos números naturales...

Vemos que ciertos conjuntos, por ejemplo $\emptyset$ es un número natural por definición explícita, ya que pertenece a todo conjunto inductivo. Igualmente, $\{\emptyset\}$ es el sucesor de $\emptyset$ y, por lo tanto, es un número natural. Análogamente, $\{\emptyset, \{\emptyset\}\}$ es el sucesor de $\{\emptyset\}$. Así, obteniendo una y otra vez el sucesor del anterior, podemos obtener otros conjuntos que son números naturales. Por comodidad les daremos nombres. Nuevamente corremos el peligro de suponer que el conjunto que tiene un nombre, por ejemplo 1, tiene las propiedades del número 1 que conocemos desde la infancia. La idea es que sí las tiene, pero eso hay que probarlo dentro de la teoría.

Notación 2.1.

$$\begin{aligned} 0 &= \emptyset \\ 1 &= S0 = \{\emptyset\} \\ 2 &= S1 = \{\emptyset, \{\emptyset\}\} \\ 3 &= S2 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \end{aligned}$$

Observe que cada uno de estos conjuntos es un número natural.

Una observación en el plano intuitivo, es que el número natural n contiene n elementos i.e. 0 no tiene elementos, 1 tiene un elemento, 2 tiene dos elementos, etc. Más aún, note que

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} \\ 2 &= \{0, 1\} \\ 3 &= \{0, 1, 2\} \\ &\vdots \end{aligned}$$

y, en general,

$$Sn = \{0, 1, \ldots, n\} ,$$

es decir, todo número natural está formado por los naturales que lo preceden.

Intuitivamente, el conjunto de los números naturales contiene a todos los conjuntos que se obtienen a partir del 0 iterando indefinidamente la operación sucesor, es decir, 0, $S0$, $SS0$ ..., pero a ningún otro.

En este punto es adecuado hacer notar que, en matemática, es habitual decir que el primer número natural es el 1. De hecho, en los años 60 y 70 de siglo pasado, esta discrepancia introdujo una suerte de controversia respecto de si el primer natural es el 0 o es el 1, ésta se produce por motivos muy superficiales que están detalladamente explicados en [**9**]. La idea es que para todos los efectos prácticos es irrelevante cuál es

el primer natural, sólo necesitamos contar con un primer natural, llámese este 0 ó 1, y cada vez que tenemos un natural, existe otro que es su sucesor inmediato. Estas son las propiedades usadas para contar y ordenar. Es más, cuando de contar se trata, resulta mejor partir en 0, ya que éste es el número de elementos dentro del conjunto vacío, 1 es un conjunto con un elemento, y como hicimos notar, cada número es un conjunto que tiene tantos elementos como su nombre (en castellano) indica. Este es el motivo por el cual los especialistas en Fundamentos de Matemática llaman cero al primer natural, bien podrían llamarle uno al conjunto vacío, dos al conjunto singleton vacío, etc., y no habría tal controversia. En la construcción que estamos haciendo es mucho más conveniente empezar por el cero, como le resultará evidente al lector una vez que termine de leer esta sección.

Teorema 2.5. *Todo número natural que es distinto de 0 es el sucesor de algún conjunto.*

Demostración. Supongamos que existe $x \in \mathbb{N}$ tal que $x \neq 0$ y para cualquier conjunto y, $x \neq Sy$. Entonces consideramos el conjunto $X = \mathbb{N} - \{x\}$. Vemos que X es inductivo. En efecto, $0 \in X$ y si $z \in X$, entonces $Sz \in \mathbb{N}$ porque $\mathbb{N}$ es inductivo. Pero, además, $Sz \neq x$, por lo tanto, $Sz \in X$. Es decir, X es inductivo. Pero esto no puede ser ya que $X \subsetneq \mathbb{N}$ y, por lo tanto, $\mathbb{N}$ no sería el menor conjunto inductivo. Como llegamos a una contradicción debemos desechar nuestra suposición, es decir, x debe ser sucesor de algún conjunto. □

La demostración que acabamos de hacer, no es sino un ejemplo de uno de los métodos más eficaces para probar propiedades de los números naturales, el Principio de Inducción. Veremos que éste no es más que aplicar adecuadamente la minimalidad de $\mathbb{N}$ entre los conjuntos inductivos.

2.1.3 El Principio de Inducción

Intuitivamente, la característica más relevante de los números naturales es que existe un primer número natural, a saber el 0, y que dado cualquier número natural n existe otro que es su sucesor inmediato, a saber Sn. Esta propiedad se traduce en un teorema que resulta ser la herramienta más importante para demostrar propiedades de los naturales, el Principio de Inducción Matemática, teorema del que derivan las propiedades que más nos interesan de estos números. En adelante nos referiremos a él simplemente como P.I.

Teorema 2.6. Principio de Inducción.
Sea B un conjunto que verifica las dos propiedades siguientes:

(i) $0 \in B$.
(ii) *Para todo n, si $n \in B$, entonces $Sn \in B$.*

Entonces $\mathbb{N} \subseteq B$.

Demostración. Basta observar que las cláusulas (i) y (ii) de la hipótesis del teorema nos dicen que B es inductivo. El teorema se obtiene porque $\mathbb{N}$ es el menor conjunto inductivo. □

El P.I. suele ser enunciado en términos de una propiedad de los números representada por una expresión $P(x)$. Como estamos hablando de conjuntos, $P(x)$ debe ser una fórmula en el lenguaje de la Teoría de Conjuntos con una variable x y que naturalmente puede contener símbolos especiales previamente definidos. En la página 138 del Capítulo 4 se entrega una definición más rigurosa de lo que debemos entender por "propiedad". En este capítulo, seguiremos con el sentido intuitivo que hemos venido usando.

Teorema 2.7. Principio de Inducción.
Consideremos una propiedad de los números naturales representada por la fórmula $P(x)$ *. Supongamos que*

(1) $P(0)$ *se verifica.*
(2) *Para todo* $n \in \mathbb{N}$ *si* $P(n)$ *se verifica, entonces* $P(Sn)$ *también se verifica.*

Entonces $P(n)$ *se verifica para todo* $n \in \mathbb{N}$.

Demostración. Consideremos el conjunto $B = \{x \in \mathbb{N} : P(x) \text{ es cierto}\}$. Entonces por (1), $0 \in B$ y si $n \in B$, por (2), $Sn \in B$, es decir, B cumple las condiciones (i) y (ii) del teorema anterior (es un conjunto inductivo) y, por lo tanto, $\mathbb{N} \subseteq B$, o lo que es lo mismo, todos los naturales verifican $P(x)$. □

Las dos maneras de enunciar el principio son equivalentes, en efecto, supongamos válida la segunda versión del P.I., aquella en términos de propiedades. Dado un conjunto B que verifica las cláusulas (i) y (ii) de 2.6, consideramos la propiedad descrita por $P(x) := x \in B$. Es claro que del Teorema 2.7 se sigue que para todo número natural n, $P(n)$ es verdadera, o sea, $\mathbb{N} \subseteq B$.

Dado que ambas versiones del teorema son equivalentes, nos referiremos a ellas indistintamente como el P.I.

Para demostrar la segunda cláusula del P.I. se procede a suponer que $n \in B$ (alternativamente, que $P(n)$ se verifica), y se argumenta para demostrar que $Sn \in B$ (alternativamente, $P(Sn)$ se verifica). Esa suposición se conoce como la *hipótesis de inducción* H.I.

Teorema 2.8. *Demostrar que si* $Sx \in \mathbb{N}$*, entonces* $x \in \mathbb{N}$.

Demostración. Supongamos que $Sx \in \mathbb{N}$ pero que $x \notin \mathbb{N}$.
Consideremos ahora el conjunto $B = \mathbb{N} - \{Sx\}$. Entonces

(i) $0 \in B$, ya que 0 no es sucesor de ningún conjunto.
(ii) Si $n \in B$ (ésta es la H.I.), entonces como $n \in \mathbb{N}$, también $Sn \in \mathbb{N}$. Queremos comprobar que $Sn \in B$. Si no, $Sn = Sx$ y por el Teorema 2.15 resulta que $x = n \in \mathbb{N}$, lo que contradice nuestra hipótesis. Luego $Sn \in B$.

Por el P.I., $\mathbb{N} \subseteq B \subsetneq \mathbb{N}$ lo que es una contradicción, luego $x \in \mathbb{N}$. □

Teorema 2.9. *Si $n \in \mathbb{N}$, entonces $n \subseteq \mathbb{N}$.*

Demostración. Lo demostraremos por inducción usando la propiedad $P(x) :=$ "si $x \in \mathbb{N}$ entonces $x \subseteq \mathbb{N}$". (Alternativamente, definimos $B = \{x \in \mathbb{N} : x \subseteq \mathbb{N}\}$ y aplicamos la versión del P.I. en términos de conjuntos).

i) Es claro que $P(0)$ se verifica porque $0 = \emptyset \subseteq \mathbb{N}$.

ii) La H.I. consiste en suponer que $P(n)$ es cierto para $n \in \mathbb{N}$. En este caso, si $n \in \mathbb{N}$, entonces $n \subseteq \mathbb{N}$. Debemos ver que esto implica que Sn verifica la condición. Para ello supongamos que $Sn \in \mathbb{N}$ y tomemos un $x \in Sn = n \cup \{n\}$. Obsérvese que por el Teorema 2.8, $n \in \mathbb{N}$. Hay, por lo tanto, dos casos: o bien $x \in n$ o bien $x = n$. En el primero, por la H.I., $x \in \mathbb{N}$; en el segundo caso $x = n \in \mathbb{N}$, en cualquier caso $x \in \mathbb{N}$, en otras palabras, si $x \in Sn$, entonces $x \in \mathbb{N}$, es decir, $Sn \subseteq \mathbb{N}$. Esto completa la demostración de $P(Sn)$ se satisface.

Aplicando el P.I. tenemos que todo número natural satisface la condición pedida.

□

Teorema 2.10. *Para todo $n \in \mathbb{N}$, si $x \in y \in n$, entonces $x \in n$.*

Para facilitar la lectura hemos escrito $x \in y \in n$ para abreviar las dos inclusiones $x \in y$ e $y \in n$.

Demostración. Por inducción usando la versión en términos de conjuntos del P.I. con el conjunto $B = \{n \in \mathbb{N} : \text{si } x \in y \in n \text{ entonces } x \in n\}$.

i) Es claro que $0 \in B$ porque el antecedente de la condición de la definición de B es siempre falso.

ii) La H.I. consiste en suponer que $n \in B$. Debemos ver que esto implica que $Sn \in B$. Para ello tomemos un $x \in y \in Sn = n \cup \{n\}$. Hay, por lo tanto, dos casos: o bien $x \in y \in n$ o bien $x \in y = n$. En el primero, por la H.I., $x \in n$; en el segundo caso también $x \in n$. En otras palabras, en cualquier caso si $x \in y \in Sn$, entonces $x \in Sn$. Esto completa la demostración de $Sn \in B$.

Aplicando el P.I. tenemos que todo número natural satisface la condición pedida.

□

Los tres teoremas anteriores tienen importancia en la estructura del orden que definiremos sobre el conjunto de los números naturales y, aún más, para posibles generalizaciones que no trataremos en este libro. Los conjuntos que satisfacen la última propiedad se dicen transitivos. El teorema entonces afirma que todo número natural es transitivo.

2.1.3 El Principio de Inducción Completa

Teorema 2.11. Principio de Inducción Completa.
Consideremos una propiedad de los números naturales representada por la fórmula $P(x)$ *. Supongamos que*

(a) $P(0)$ *se verifica.*

(b) *Si* $P(k)$ *se verifica para todo* $k \subseteq n$*, entonces* $P(Sn)$ *también se verifica.*

Entonces para todo $n \in \mathbb{N}$*, se verifica* $P(n)$*.*

Este principio es también llamado *inducción por curso de valores* porque no basta con comprobar que si la propiedad se verifica para un número, entonces también se verifica para el sucesor (como es el caso del P.I.), sino que se debe ver que si la propiedad se cumple para todos los números menores que uno dado n, entonces ella también se aplica a n. En apariencia este principio es más débil que el P.I. ya que hay que comprobar más cosas para obtener el mismo resultado. Veremos en la próxima sección que no es así, ambos principios son equivalentes.

Demostración. Consideremos una propiedad definida por la fórmula $P(x)$ y supongamos que para ella se cumplen las condiciones (a) y (b) del P.I.C.

Aplicaremos ahora el P.I. a la nueva propiedad definida por $Q(x) :=$ "para todo $y \subseteq x$ se verifica $P(y)$" para demostrar que para todo $n \in \mathbb{N}$ se cumple $Q(n)$.

- Vemos primero que $Q(0)$ significa que para cualquier m,

  $$\text{si } m \subseteq 0, \text{ entonces } P(m) .$$

  Esta afirmación es trivialmente cierta ya que, si $m \subseteq 0$, entonces $m = 0$ y por (a), $P(0)$ es cierta.
- Supongamos que $Q(n)$ se verifica.Entonces $P(m)$ es verdadero para todo $m \subseteq n$, pero este es el antecedente de la implicación (b) de P.I.C., luego también debe ser verdadero su consecuente, a saber, $P(Sn)$. O sea tenemos que se verifica $P(m)$ para todo $m \subseteq Sn$, en otras palabras, se verifica $Q(Sn)$. En resumen, hemos demostrado que suponiendo $Q(n)$ podemos probar $Q(Sn)$.

Los dos pasos anteriores son precisamente las dos hipótesis (i) y (ii) del P.I. y en virtud de éste podemos concluir que para todo $n \in \mathbb{N}$, $Q(n)$ es válido. Pero, entonces, con mayor razón $P(n)$ es válido ya que $Q(n)$ lo incluye.

Esto completa nuestra demostración: a partir de (a) y (b) usando el P.I., hemos demostrado que $P(n)$ es cierta para todo $n \in \mathbb{N}$. □

El principio de Inducción Completa también puede plantearse en términos de la relación de pertenencia.

Teorema 2.12. *Sea* $B \subseteq \mathbb{N}$ *tal que*

i) $0 \in B$

ii) *Si* $\{k \in \mathbb{N} : k < n\} \subseteq B$, *entonces* $n \in B$.

Entonces $B = \mathbb{N}$.

2.1.4 Los axiomas de Peano

Hemos visto que 0 es un número natural y que el sucesor de un natural también lo es. Esto, junto a los Teoremas 2.13, 2.15 y 2.7, que demostraremos a continuación, constituyen los conocidos Axiomas de Peano para los números naturales.

Teorema 2.13. *0 no es el sucesor de ningún conjunto.*

Demostración. Basta ver que para todo conjunto x se tiene $x \in Sx$, es decir, $Sx \neq \emptyset = 0$. □

Lema 2.14. *Para todo número natural* n, $\bigcup(Sn) = n$.

Demostración. Supongamos que $x \in \bigcup(Sn)$, es decir, $x \in y \in Sn$ para algún y. Entonces como $y \in n$ o bien $y = n$, en cualquier caso, por el Ejercicio 2.10, $x \in n$. Esto demuestra que $\bigcup(Sn) \subseteq n$.

Ahora bien, si $x \in n$, entonces $x \in n \in n \cup \{n\}$, luego $x \in \bigcup(Sn)$, lo que completa la demostración. □

El siguiente teorema nos dice que si pensamos la operación de tomar el sucesor de un conjunto como una función entre ciertos conjuntos, ésta es inyectiva.

Teorema 2.15. *Si* $Sx = Sy$, *entonces* $x = y$.

Demostración. Supongamos que $Sx = Sy$. Entonces, por el lema anterior, tenemos $x = \bigcup(Sx) = \bigcup(Sy) = y$. □

2.1.5 Orden

Resulta interesante notar que

$$0 \in 1 \in 2 \in 3 \in \cdots \quad \text{y también} \quad 0 \subseteq 1 \subseteq 2 \subseteq 3 \cdots$$

Esta observación nos da la intuición que la relación de pertenencia entre naturales define una noción de orden apropiada. En estricto rigor es al revés, los números naturales se definen así *para* que la relación de pertenencia sea un orden con buenas propiedades.

Definición 2.16. La relación $<$ se define en $\mathbb{N}$ por:

$$m < n \quad \text{si y solo si} \quad m \in n \ .$$

Denotaremos $m \leq n$ y diremos que m es menor o igual que n si $m \in n$ o bien $m = n$.

Lema 2.17. *Para todo $n, m \in \mathbb{N}$,*

1. $0 \leq n$.
2. *Si $x \in n$, entonces $x \in \mathbb{N}$.*
3. $m < Sn$ *si y solo si* $m \leq n$.
4. *Si $n < m$, entonces $Sn \leq m$.*

Demostración.
1. Por inducción con la propiedad definida por $P(x) :=$ "$0 \leq x$".
   - $P(0)$ se verifica.
   - Supongamos ahora que $P(n)$ se verifica.

Es decir, $0 \leq n$, o sea $0 \in n$ ó $0 = n$. En cualquier caso $0 \in n \cup \{n\} = Sn$, o sea $P(Sn)$ se verifica.

Luego, en virtud del P.I., para todo $n \in \mathbb{N}$, $0 \leq n$.

2. Por inducción sobre n. La propiedad está definida por la fórmula $P(x) :=$ "para todo y, si $y < x$, entonces $y \in \mathbb{N}$", que nos dice que $x \subseteq \mathbb{N}$.
   - $P(0)$ se verifica trivialmente porque no existe ningún número menor que 0.
   - Supongamos $P(n)$, o sea, $n \subseteq \mathbb{N}$. Para demostrar $P(Sn)$ debemos tomar un $y \in Sn$. Entonces $y \in n$ ó $y = n$.

Si $y \in n$, por hipótesis de inducción, $y \in \mathbb{N}$.

Si $y = n$, entonces $y \in \mathbb{N}$. En cualquier caso $y \in \mathbb{N}$. Luego $Sn \subseteq \mathbb{N}$ y por el P.I., todo $n \in \mathbb{N}$ verifica $P(n)$.

3.

$m < Sn$ si y solo si $m \in Sn = n \cup \{n\}$ si y solo si $m \leq n$.

4.

Por inducción sobre m. Consideramos la propiedad definida por $P(x) :=$ "para todo y, si $y < x$, entonces $Sy \leq x$."

- $P(0)$ se verifica trivialmente como en el caso anterior.
- Supongamos $P(m)$.

  Supongamos pues que $y < Sm$ y recordemos que por 3, esto ocurre si y solo si $y \in m$ o $y = m$.

Si $y \in m$, por hipótesis de inducción, $Sy \leq m$ y luego $Sy \leq Sm$.

Si $y = m$, entonces $Sy = Sm$. En cualquier caso, si $y < Sm$, entonces $Sy \leq Sm$, es decir, $P(Sm)$ se verifica. Luego por el P.I., para todo $m \in \mathbb{N}$, $P(m)$ se verifica.

□

Debemos demostrar que relación $\leq$ es efectivamente una relación de orden y que tiene ciertas propiedades adicionales.

Teorema 2.18. *La relación* $\leq$ *es un orden total sobre* $\mathbb{N}$.

Demostración.

1. La relación $\leq$ es obviamente reflexiva.

2. La relación $\leq$ es antisimétrica. En efecto, supongamos que $m \leq n$ y $n \leq m$, pero $m \neq n$. Entonces $m \in n$ y $n \in m$. Al final de esta demostración probaremos por inducción que esto no es posible.

3. La relación $\leq$ es transitiva. Supongamos que $k \leq m$ y $m \leq n$. Demostraremos que $k \leq n$ por inducción sobre n. Para ello sea

$P(x) :=$ "para todo y y para todo z, si $z \leq y$ e $y \leq x$, entonces $z \leq x$."

- $P(0)$ se verifica ya que si $k \leq m$ y $m \leq 0$, $m = 0$ luego $k \leq 0$.
- Si $P(n)$ se verifica, consideremos $k \leq m$ y $m \leq Sn$. Entonces $m < Sn$ ó $m = Sn$.

Si $m < Sn$, entonces por el Lema 2.17,3, $m \leq n$ y por hipótesis de inducción $k \leq n$. Es decir, $k \in n$ ó $k = n$. En cualquier caso, $k \in Sn$, o sea, $k \leq Sn$.

Si $m = Sn$, como $k \in m$ ó $k = m$, tenemos $k \in Sn$ ó $k = Sn$, es decir, $k \leq Sn$.

Esto completa la inducción, luego todo número natural n verifica $P(n)$, o sea, $\leq$ es transitiva.

4. La relación $\leq$ es un orden total. Sean m y n dos números naturales. Demostraremos por inducción sobre n que $m < n$ ó $m = n$ ó $n < m$. La propiedad deseada queda descrita por

$P(x) :=$ "para todo y, $y < x$ ó $y = x$ ó $x < y$".

- $P(0)$ se verifica por el Lema 2.17 1.
- Supongamos $P(n)$ se verifica. Entonces para todo m, $m < n$ ó $m = n$ ó $n < m$.

Si $m < n$ ó $m = n$, entonces $m \in Sn$, luego $m < Sn$. Si $n < m$, entonces $Sn \leq m$ por el Lema 2.17, 4.

Luego por P.I., $\leq$ es un orden total sobre $\mathbb{N}$.

Por último, vemos que para dos números naturales n y m sólo se puede verificar una de las tres posibilidades. De lo contrario, existirían números naturales n y m tales que o bien $n \in n$ o bien $n \in m \in n$. Por inducción, ninguna de éstas es posible.

Usemos la propiedad dada por $P(x) :=$ "$x \notin x$".

Es claro que $P(0)$ se verifica por que $0 \notin 0 = \emptyset$.

Supongamos entonces que $P(n)$ se verifica y que $Sn \in Sn = n \cup \{n\}$. Hay dos casos, el primero es $Sn \in n$. En este caso tenemos $n \in Sn \in n$ y por el Teorema2.10, concluimos que $n \in n$, lo que contradice la hipótesis de inducción.

El segundo caso es $Sn = n$, y volvemos a obtener $n \in n$.

Vemos entonces que ambos casos son contradictorios y que, por lo tanto, $Sn \notin Sn$, confirmando que se verifica $P(Sn)$.

En virtud del P.I., para todo número natural n, se tiene $n \notin n$.

Para verificar por inducción que no existen números naturales n y m tales que $n \in m \in n$ usemos la propiedad dada por $P(x) :=$ "no existe un natural n tal que $n \in x \in n$".

Es inmediato que 0 sí verifica esta propiedad por que si no, existiría un n tal que $n \in 0 = \emptyset$.

Supongamos entonces que $P(m)$ se verifica y veamos qué sucede con Sm. Si $P(Sm)$ fuese falsa, entonces existiría un n tal que $n \in Sm \in n$.

Obsérvese que $Sm \in n$ implica que $m \in n$. Hay dos casos. Si $n \in m$, tendríamos que $n \in m \in n$. Si $m = n$, tedríamos que $m \in m$. En ambos casos se contradice la H.I. □

La propiedad demostrada en el punto 4 del teorema anterior suele ser llamada *ley de tricotomía*.

Un orden se dice *discreto* si todo elemento tiene un sucesor inmediato, es decir, para todo a existe b tal que $a < b$ y si $a \leq c \leq b$, entonces o bien $c = a$ o bien $c = b$. Equivalentemente, podemos decir, b es el sucesor inmediato de a si no existe un elemento c tal que $a < c < b$.

Teorema 2.19. *La relación $\leq$ es un orden discreto sobre $\mathbb{N}$.*

Demostración. Para demostrar que el orden de los naturales es discreto, veremos que dado cualquier $n \in \mathbb{N}$, su sucesor Sn es efectivamente el sucesor inmediato de n.

Supongamos que existe $c \in \mathbb{N}$ tal que $n < c < Sn$. Entonces, $c \in n \cup \{n\}$ y como $c \neq n$, $c \notin \{n\}$, luego $c \in n$. Pero esto nos dice que $c < n < c$ lo que por antisimetría implica $n = c$, contradiciendo nuestra hipótesis. □

2.1.6 Los naturales están bien ordenados

Recordemos que un conjunto totalmente ordenado $(A, \preceq)$ se dice bien ordenado (ver página 48 del Capítulo 1) si todo subconjunto no vacío de A tiene un elemento mínimo. En tal caso decimos que $\preceq$ es un buen orden. Que el orden de los números naturales sea un buen orden es la principal característica de los naturales. Más aún, en buena medida, el orden de los naturales da origen al concepto de buen orden.

Teorema 2.20. *La relación $\leq$ es un buen orden.*

Demostración.
Hemos visto que $\leq$ es un orden total. Debemos demostrar que si $X \subseteq \mathbb{N}$ y $X \neq \emptyset$, entonces X tiene un menor elemento.

Para ello suponemos que X no tiene menor elemento y aplicamos el Principio de Inducción Completa 2.12 al conjunto $B = \mathbb{N} - X$.

Es claro que $0 \notin X$, pues si no, 0 sería el menor elemento de X, o sea, $0 \in \mathbb{N} - X$.

Dado n, si para todo $k < n$, $k \in \mathbb{N} - X$, entonces $n \in \mathbb{N} - X$ porque, si no, $n \in X$ y n sería el menor elemento de X, luego $\mathbb{N} - X = \mathbb{N}$, es decir, $X = \emptyset$, lo que es una contradicción. Por lo tanto, todo subconjunto no vacío de $\mathbb{N}$ tiene un menor elemento y, por lo tanto, $\leq$ es un buen orden. □

El teorema anterior es conocido como el principio del buen orden y es equivalente al Principio de Inducción.

Teorema 2.21. *Los siguientes son equivalentes.*

1. *Principio de Inducción (P.I.).*
2. *Principio de Inducción Completa (P.I.C.).*
3. *Principio del Buen Orden (P.B.O.).*

Demostración. $1 \Rightarrow 2$.
Esto se demostró en el Teorema 2.11.
$2 \Rightarrow 3$.
Esto se demostró en el Teorema 2.20.
$3 \Rightarrow 1$.
Supongamos el P.B.O. Supongamos además que $P(x)$ es una propiedad que verifica las dos hipótesis del P.I., es decir, $P(0)$ es cierta y si $P(n)$ es cierta, entonces $P(Sn)$ también lo es.

Formamos el conjunto $B = \{x \in \mathbb{N} : P(x) \text{ es falso}\}$. Es claro que $B \subseteq \mathbb{N}$. Si $B \neq \emptyset$, entonces B tiene un menor elemento; llamémoslo m. Es claro que $m \neq 0$ porque $P(0)$ es cierto por hipótesis.

Entonces $m \neq 0$ y, por lo tanto, $m = Sr$ para algún número natural r. Por otra parte, como m es el elemento mínimo de B y $r < m$, $r \notin B$, es decir, $P(r)$ es verdadero, pero entonces la hipótesis (ii) nos dice que $P(Sr)$, o sea, $P(m)$ es cierto, en contradicción con la definición de m. La única posibilidad es que el conjunto B sea vacío, y, por lo tanto, que todo natural n verifique la propiedad definida por $P(x)$.
□

Teorema 2.22. *Si un subconjunto no vacío de $\mathbb{N}$ tiene una cota superior, entonces tiene un máximo elemento.*

Demostración.
Sea $X \subseteq \mathbb{N}$, $X \neq \emptyset$ y acotado superiormente, definimos

$$Y = \{x \in \mathbb{N} : x \text{ es cota superior de } X\}.$$

Por hipótesis $Y \neq \emptyset$. Sea m el menor elemento de Y. Debemos demostrar que $m \in X$.

Si $m = 0$, entonces para todo $x \in X$, $x \leq 0$, o sea $X = \emptyset$ o bien $X = \{0\}$. El primer caso no ocurre por hipótesis y en el segundo, 0 es el máximo de X.

Si $m \neq 0$, entonces $m = Sn$ para algún n. Pero entonces si $m \notin X$, n es cota superior de X y $n < m$, una contradicción. Luego $m \in X$ y es el mayor elemento de X. □

2.1.7 Operaciones con Números Naturales

Definiremos ahora la suma y la multiplicación de números naturales usando un procedimiento muy importante en matemática, el de las definiciones recursivas. En estricto rigor deberíamos demostrar primero que se puede hacer definiciones recursivas. Esto escapa a los objetivos de este libro.

Consideremos las siguientes definiciones.

$$\begin{cases} n+0 &= n \\ n+S(m) &= S(n+m) \end{cases} \qquad \begin{cases} n\cdot 0 &= 0 \\ n\cdot S(m) &= n\cdot m+n \end{cases}$$

La idea es que, para sumar digamos $4+3$, de acuerdo con la segunda condición de la definición de suma, como 3 es el sucesor de 2, debemos primero saber cómo se suma $4+2$, a su vez, para saber esto, debemos saber cuánto es $4+1$ y similarmente, cuánto es $4+0$. Pero esto último está definido por la primera condición de la definición, a saber, $4+0=4$. En general, para sumar o multiplicar un número con otro, debemos primero saber el resultado de sumar (o multiplicar) el predecesor, el predecesor del predecesor y así sucesivamente hasta que se llega al cero que no tiene predecesor. Sin embargo, este caso queda cubierto por la primera condición de la definición.

Debemos insistir que esta es una definición dentro de la teoría de conjuntos y que no podemos suponer ninguna propiedad de las operaciones, por ejemplo, conmutatividad, distributividad, etc., sin antes demostrarla usando sólo aquello que está permitido dentro de la teoría. La herramienta principal aquí es el Principio de Inducción.

Lema 2.23. *Las siguientes son algunas de las propiedades de la suma y de la multiplicación de números naturales.*

1. *Para todo* $n\in\mathbb{N}$, $0+n=n$.
2. *Para todo* $n\in\mathbb{N}$, $n+1=Sn$.
3. *Para todo* $n\in\mathbb{N}$, $1\cdot n=n$.
4. *Para todo* $n\in\mathbb{N}$, $1+n=n+1$.

Demostración.
1. Lo demostraremos por inducción sobre n. Consideramos la propiedad $P(x) :=$ "$0+x=x$". En primer lugar, vemos que en virtud de la primera condición de la definición de suma, $0+0=0$, es decir, $P(0)$ es verdad, o sea, se cumple el primer paso de la inducción.

Supongamos ahora nuestra hipótesis de inducción, es decir, $0+n=n$. Entonces, por la segunda condición de la definición, $0+Sn=S(0+n)=Sn$, es decir, $P(Sn)$ es verdad, lo que completa nuestra inducción y la propiedad es verdadera para todo natural n.

2. Como por definición $1=S0$, $n+1=n+S0=S(n+0)=Sn$. Obsérvese que esta demostración usa ambas cláusulas de la definición de suma, pero no utiliza inducción.

4. Por inducción sobre n.

Vemos que $1+0=1=0+1$, luego la propiedad vale para $n=0$.

Supongamos que $1 + n = n + 1$ y calculemos

$$1 + Sn = S(1 + n) = S(n + 1) = (n + 1) + 1 = Sn + 1\,,$$

o sea, la propiedad vale para Sn. Luego por P.I., vale para todo $n \in \mathbb{N}$.

□

Teorema 2.24. *Las siguientes son algunas de las propiedades de la suma y de la multiplicación de números naturales.*

1. *La suma y la multiplicación son asociativas.*
2. *La suma y la multiplicación son conmutativas.*
3. *La multiplicación distribuye sobre la suma.*
4. *Si $mn = 0$ entonces o bien $n = 0$ o bien $m = 0$. Decimos que en los números naturales no hay* divisores del cero*.*

Demostración.
1. Lo haremos para la suma, la demostración de la asociatividad de la multiplicación es similar. Queremos ver que para tres números p, m, $n \in \mathbb{N}$, $(p+m)+n = p+(m+n)$. Haremos inducción sobre n .

Si $n = 0$, entonces $(p + m) + 0 = p + m = p + (m + 0)$, y la propiedad se cumple para $n = 0$.

Supongamos que $(p + m) + n = p + (m + n)$. Entonces

$$\begin{aligned}
(p + m) + Sn &= S((p + m) + n) && \textit{definición de suma},\\
&= S(p + (m + n)) && \textit{H.I.},\\
&= p + S(m + n) && \textit{definición de suma},\\
&= p + (m + Sn) && \textit{definición de suma},
\end{aligned}$$

es decir, la propiedad vale para Sn. Luego por el P.I., vale para todo $n \in \mathbb{N}$.

La asociatividad de la multiplicación se demuestra de manera análoga.

2. Debemos demostrar que para todo n, $m \in \mathbb{N}$, $n + m = m + n$. Por inducción sobre n. Consideramos $P(x) :=$ "$m + n = n + m$", donde m es fijo.

$P(0)$ se cumple porque $m + 0 = m = 0 + m$. Obsérvese que la primera identidad es por la definición de suma y la segunda es por el Lema 2.23,1.

Supongamos ahora que $m + n = n + m$. Entonces

$$\begin{aligned}
m + Sn &= m + (n + 1) && Sn = n + 1,\\
&= (m + n) + 1 && \textit{asociatividad de la suma},\\
&= (n + m) + 1 && \textit{H.I.},\\
&= n + (m + 1) && \textit{asociatividad de la suma},\\
&= n + (1 + m) && \textit{Lema } 2.23{,}4,\\
&= (n + 1) + m && \textit{asociatividad de la suma},\\
&= Sn + m && Sn = n + 1,
\end{aligned}$$

lo que prueba que $P(Sn)$ vale. Por el P.I., la propiedad vale para todo $n \in \mathbb{N}$.

La conmutatividad de la multiplicación se demuestra de manera análoga.

3. Para probar la distributividad haremos inducción para el número x con la propiedad $P(x) :=$ "$(p+m)\cdot x = p\cdot x + m\cdot x$".

Para $x = 0$ la propiedad se reduce a la definición de multiplicar por 0, a saber,

$$(p+m)\cdot 0 = 0 = 0+0 = p\cdot 0 + m\cdot 0\,.$$

Supongamos entonces que la propiedad vale para x. Entonces

$$\begin{array}{rcll} (p+m)\cdot Sx & = & (p+m)\cdot x + (p+m) & \textit{definición de producto},\\ & = & (p\cdot x + m\cdot x) + (p+m) & \textit{H.I.},\\ & = & (p\cdot x + p) + (m\cdot x + m) & \textit{asoc. y conmut. de la suma},\\ & = & p\cdot Sx + m\cdot Sx & \textit{definición de producto}, \end{array}$$

es decir, la propiedad vale para Sx. Luego por el P.I., vale para todo $n \in \mathbb{N}$.

4. Sean $m \neq 0$ y $n \neq 0$. Entonces $m = x+1$ y $n = y+1$ para ciertos números naturales x e y y por lo tanto

$$m\,n = (x+1)(y+1) = x\,y + x + y + 1 = S(x\,y + x + y)\,,$$

por distributividad y asociatividad (de hecho esta última nos permite escribir la expresión $x\,y + x + y$ sin paréntesis), o sea, $x\,y + x + y \in m\,n$ y, por lo tanto, este último conjunto es no vacío, o sea, $m\,n \neq 0$. □

El siguiente teorema nos indica cómo podemos definir la resta de dos números naturales cuando esto es posible, es decir, si uno es mayor que el otro.

Teorema 2.25. *Si $m \leq n$, entonces existe un único número natural d tal que $n = m + d$.*

El recíproco también es cierto, es decir, si para algún d, $m = m + d$, entonces $m \leq n$.

Demostración. Lo probaremos por inducción sobre n. La condición a probar está dada por la propiedad

$P(n) :=$ "para todo m, si $m \leq n$, entonces existe un d tal que $m + d = n$".

Vemos primero que si $m \leq 0$ entonces $m = 0$ luego haciendo $d = 0$, tenemos $m + d = 0 + 0 = 0 = n$, es decir, la propiedad vale para 0.

Supongamos ahora nuestra hipótesis de inducción y consideremos un número natural $m \leq Sn$. Hay dos casos o bien $m \leq n$ o bien $m = Sn$.

En el primer caso $m \leq n$ y por la H.I., existe d' tal que $m + d' = n$, luego

$$Sn = S(m + d') = m + Sd'\,,$$

o sea, $d = Sd'$ es el número buscado.

En el segundo caso $m = Sn$, entonces $Sn = m + 0$. Vemos que en cualquier caso, la propiedad vale para Sn, luego por el P.I. la propiedad vale siempre.

Falta verificar que este número d es único. Para ello, como es habitual, suponemos que hay dos soluciones y probamos que deben ser iguales. Consideremos entonces dos números naturales $m \leq n$ y supongamos que $n = m + d = m + d'$, entonces por la ley de cancelación para la suma, la que será demostrada en la sección 1.a del siguiente teorema, $d = d'$.

Para probar el recíproco hacemos inducción sobre d usando la propiedad definida por $P(d) :=$ "$m \leq m + d$".

Si $d = 0$, entonces la propiedad se cumple.

Supongamos como H.I. que es cierto que $m \leq m + d$. Entonces $m + Sd = S(m + d) > m + d \geq m$. Es decir, Sd verifica la propiedad. Luego por el P.I. ésta es válida para todo d. □

Terminamos esta sección con un teorema en el que se resumen las principales reglas de cancelación para las operaciones con números naturales.

Teorema 2.26. *Las siguientes leyes de cancelación valen para números naturales m, n y r.*

1. *a) Si $m + r = n + r$, entonces $m = n$.*
   b) Supongamos que $r \neq 0$. Entonces, si $m\,r = n\,r$, entonces $m = n$.
2. *a) $m \leq n$ si y solo si $m + r \leq n + r$.*
   b) Si $r > 0$, entonces $m \leq n$ si y solo si $m\,r \leq n\,r$.
   La relación $\leq$ puede reemplazarse por $<$.

Demostración.

1.a) Por inducción sobre r. La propiedad es

$P(r) :=$ "para todo m y para todo n, si $m + r = n + r$, entonces $m = n$".

Para $r = 0$, la propiedad es evidente.

Consideremos verdadera la hipótesis de inducción para r, o sea, que para cualquier par de números naturales, si $m + r = n + r$, entonces $m = n$. Ahora supongamos que $m + Sr = n + Sr$, entonces

$$S(m + r) = m + Sr = n + Sr = S(n + r)\,,$$

pero entonces $m + r = n + r$, porque sus sucesores son iguales. Aplicando la hipótesis, $m = n$. Luego por el P.I. la propiedad se cumple para todo número natural.

1.b) La ley de cancelación para el producto está definida por la propiedad

$P(r) :=$ "para todo m y para todo n, si $r \neq 0$ y $m\,r = n\,r$, entonces $m = n$".

Haremos nuestra inducción sobre r comenzando con $r = 1$. Es claro que la propiedad es inmediata en este caso ya que $m = m \cdot 1 = n \cdot 1 = n$.

Consideremos válida la hipótesis de inducción y supongamos que $m \cdot Sr = n \cdot Sr$. Podemos suponer sin pérdida de generalidad que $m \leq n$. Por la definición del producto,

$$m\,r + m = m \cdot Sr = n \cdot Sr = n\,r + n\,.$$

Entonces

$$
\begin{aligned}
mr + m &= nr + n \\
mr + m &= (m + d)r + (m + d) && m \leq n \text{ y } \textit{Teorema } 2.25, \\
mr + m &= (mr + dr) + (m + d) && \textit{distributividad}, \\
mr + m &= mr + (dr + (m + d)\,) && \textit{asociatividad}, \\
m &= dr + (m + d) && \textit{cancelación}, \\
m &= m + (dr + d) && \textit{asociatividad y conmutatividad}, \\
0 &= dr + d && \textit{cancelación}, \\
0 &= d \cdot Sr && \textit{definición de producto},
\end{aligned}
$$

pero como $Sr \neq 0$, por Teorema 2.24, 4, la única posibilidad es que $d = 0$.

2.a) Si $m \leq n$ entonces $n = m + d$ para cierto d y entonces $n + r = (m + d) + r = (m + r) + d$ por asociatividad y conmutatividad. Entonces $mr \leq nr$ por el Teorema 2.25 (recíproco). La otra dirección es simplemente la cancelación de 1.a.

2.b) Supongamos que $r > 0$. Entonces $nr = (m+d)r = mr+dr$ por distributividad. Entonces $mr \leq nr$ por el Teorema 2.25 (recíproco).

La otra dirección es simplemente la cancelación de 1.b. □

2.1.8 Ejercicios

1. Demuestre:
   a) Decida si son ciertas o falsas las afirmaciones siguientes:

   (i) $1 \in 2$ (ii) $1 \cap 2 = 0$ (iii) $(0 \cap 2) \in 1$
   (iv) $1 \subseteq 2$ (v) $1 \cup 2 = 2$ (vi) $\bigcup 3 \subseteq 3$
   (vii) $\bigcap 4 \in 4$

   b) Muestre que los siguientes conjuntos son números naturales.

   $$\bigcup \emptyset\,,\ \mathcal{P}(\emptyset)\,,\ \bigcup(\bigcup \emptyset)\,,\ \mathcal{P}(\mathcal{P}(\emptyset))\,,\ \bigcup(\bigcup(\bigcup \emptyset))\,,\ \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))).$$

   Expréselos usando los conjuntos 0, 1, 2, 3 y 4.
   c) Si $A = \{\{2, 3\}, 4, \{4\}\}$, encontrar $\bigcap(\bigcup A - 4)$.
   d) Construya $\bigcap\bigcup(\mathcal{P}(2) - 2)$.
   e) Si $A = \{\{1, 2\}, \{2, 0\}, \{1, 3\}\}$, construya:

   $$\bigcup A\,,\ \bigcap A\,,\ \bigcup(\bigcup A)\ ,\ \bigcap(\bigcap A)\,,\ \bigcup(\bigcap A)\,,\ \bigcap(\bigcup A).$$

2. Demuestre que la intersección de un conjunto no vacío de números naturales es, a su vez, un número natural. Enseguida demuestre que éste es el menor elemento del conjunto.

   Ésta es una demostración alternativa de que los números naturales están bien ordenados por la inclusión.
3. Sea $\{a_i : i \in \mathbb{N}\}$ una familia de conjuntos tal que $a_i \subseteq a_{Si}$, para todo $i \in \mathbb{N}$. Probar que $a_0 \subseteq a_n$ para todo $n \in \mathbb{N} - \{0\}$.
4. Probar que si $n \in \mathbb{N}$, $\bigcup Sn = n$ y que $\bigcup \mathbb{N} = \mathbb{N}$.
5. Probar que si $a \subseteq \mathbb{N}$, $a \neq \emptyset$ y $\bigcup a = a$, entonces $a = \mathbb{N}$.
6. Probar que si m y n están en $\mathbb{N}$ y $m \neq n$, entonces:
   a) $m \cup n = \begin{cases} m & \text{si } n \in m, \\ n & \text{si } m \in n. \end{cases}$

b) $m \cap n = \begin{cases} n & \text{si } n \in m, \\ m & \text{si } m \in n. \end{cases}$

7. Probar que si $n \in m$ y $n \neq 0$, entonces existe un mayor elemento en n.
8. Si $a \subseteq b \subseteq \mathbb{N}$ son no vacíos, n es el menor elemento de a y m es el menor elemento de b, ¿cuál es la relación entre n y m? Justificar y responder la pregunta análoga para los mayores elementos de a y de b si estos existen.
9. Probar que si n y m están en $\mathbb{N}$ y $n < m$, entonces $Sn < Sm$.
10. Probar que no existe una función $F : \mathbb{N} \longrightarrow \mathbb{N}$ tal que para todo $n \in \mathbb{N}$, $F(Sn) < F(n)$.
11. Probar que si $P(x)$ define una propiedad y existe un $k_0 \in \mathbb{N}$, tal que
    a) $P(k_0)$ se verifica y
    b) para todo $n \in \mathbb{N}$ tal que $k_0 \leq n$, si se verifica $P(n)$ entonces se verifica $P(Sn)$,

    entonces $P(n)$ se verifica para todo $n \geq k_0$.

2.2 Los Números Enteros

A partir de los números naturales de la sección anterior, construiremos ahora el conjunto $\mathbb{Z}$ de los números enteros. Estos resultarán ser clases de equivalencia de pares ordenados de números naturales, es decir, conjuntos muy complicados. Esta construcción se debe a A. Grothendieck y es muy ingeniosa si bien algo artificial. Sin embargo, hay ciertas intuiciones básicas de los números enteros que pueden motivarla.

En los números naturales a veces se puede definir la resta y a veces no. Si $n \geq m$, entonces tiene sentido definir la diferencia o resta $n - m$ como aquel único natural d tal que $n = m + d$, o sea aquel número que sumado al menor nos da el mayor. En el Teorema 2.25 hemos probado que tal número existe. Una constante en el trabajo con los números enteros es que recurriremos una y otra vez a los teoremas acerca de los números naturales ya demostrados en la sección anterior.

Podemos pensar, siguiendo nuestras naturales intuiciones, que los enteros negativos pueden resultar de "restar" un natural mayor de uno menor. Por ejemplo, el entero negativo -5 resulta de "restar" 5 de 0, porque por analogía con la definición anterior, -5 sería el "número" que sumado a 5 nos da 0. Hemos escrito restar entre comillas porque tal operación es una intuición que no está definida en esta situación.

Entonces nos damos cuenta del siguiente hecho: si -5 es el "número"que sumado al 5 nos da 0, entonces también -5 es el "número" que sumado al 6 nos da 1 y -5 es el "número" que sumado al 7 nos da 2, etc.

En general, si trabajamos con números enteros donde la resta está bien definida, se tiene que

$$n - m = p - q \quad \text{si y solo si} \quad n + q = p + m\,.$$

Esta observación es el origen de la construcción que haremos a continuación.

Sea R la relación definida sobre $\mathbb{N} \times \mathbb{N}$, el conjunto de los pares ordenados de números naturales, definida por

$$(n, m)\, R\, (p, q) \quad \text{si y solo si} \quad n + q = p + m\,.$$

Teorema 2.27. *R es una relación de equivalencia.*

Demostración. Como $n + m = n + m$, $(n, m)\, R\, (n, m)$, o sea, R es reflexiva.

Por definición R es obviamente simétrica.

Para verificar la transitividad, supongamos que $(n, m)\, R\, (p, q)$ y que $(p, q)\, R\, (r, s)$. Entonces $n + q = p + m$ y $p + s = r + q$. Sumando $r + s$ a la primera de estas ecuaciones tenemos

$$\begin{array}{rcll}
(n+q)+(r+s) & = & (p+m)+(r+s) & \textit{sumando } r+s \textit{ a ambos lados},\\
n+(q+(r+s)\,) & = & p+(m+(r+s)\,) & \textit{asociatividad en } \mathbb{N},\\
n+(\,(q+r)+s) & = & p+(\,(m+r)+s) & \textit{asociatividad en } \mathbb{N},\\
n+(s+(q+r)\,) & = & (p+(m+r)\,)+s & \textit{conmutat. y asociat. en } \mathbb{N},\\
(n+s)+(q+r) & = & (\,(m+r)+p)+s & \textit{conmutat. y asociat. en } \mathbb{N},\\
(n+s)+(r+q) & = & (m+r)+(p+s) & \textit{conmutat. y asociat. en } \mathbb{N},\\
(n+s)+(r+q) & = & (m+r)+(r+q) & \textit{porque } p+s=r+q,
\end{array}$$

luego podemos cancelar $r + q$ en la última línea obteniendo $n + s = r + m$, o sea, $(m, n)\, R\, (r, s)$, que es lo que queríamos demostrar. □

Si denotamos $[(n, m)]_R$ a la clase de equivalencia del par (n, m), entonces definimos el conjunto $\mathbb{Z}$ de los *números enteros*

$$\mathbb{Z} = \{\, [(n, m)]_R \;:\; n, m \in \mathbb{N}\}\,.$$

Para no hacer la lectura tan complicada, simplificaremos la notación eliminando el subíndice R de modo que $[(n, m)]_R$ en adelante lo escribiremos $[(n, m)]$.

2.2.1 Orden

Queremos definir un orden sobre los números enteros que refleje el que conocemos. Veamos un ejemplo que ilustra una sutil dificultad que se presenta al trabajar con clases de equivalencia, lo que nos obliga a ser cuidadosos.

Supongamos que se define la siguiente relación sobre $\mathbb{Z}$:

$$[(n, m)] \;\simeq\; [(p, q)] \quad \text{si y solo si} \quad n + m \leq p + q\,.$$

Entonces, tenemos que $[(1, 3)] = [(8, 10)]$, porque $(1, 3)\ R\ (8, 10)$ y análogamente $[(13, 14)] = [(5, 6)]$ porque $(13, 14)\ R\ (5, 6)$. Por otra parte $[(1, 3)] \simeq [(13, 14)]$ pero, sin embargo, no se verifica que $[(8, 10)] \simeq [(5, 6)]$, en otras palabras, la relación $\simeq$ no está bien definida porque dependiendo de los representantes de las clases $[(n, m)]$ que se use, éstas estarán o no relacionadas. Esto lo debemos evitar. Siempre que definamos relaciones u operaciones entre clases de equivalencia por medio de algún

representante, debemos verificar que ella no depende de esos representantes; en tal caso decimos que la relación u operación está *bien definida*.

Los número enteros pueden ser ordenados de la siguiente manera:

$$[(n,m)] <_{\mathbb{Z}} [(p,q)] \quad \text{si y solo si} \quad n+q < p+m\,.$$

Obsérvese que la primera relación, $<_{\mathbb{Z}}$, es entre números enteros y la segunda, $<$, es entre números naturales. Usaremos también la notación

$$\begin{aligned}[(n,m)] \leq_{\mathbb{Z}} [(p,q)] \quad &\text{si y solo si} \quad [(n,m)] <_{\mathbb{Z}} [(p,q)] \quad \text{ó} \quad [(n,m)] = [(p,q)] \\ &\text{si y solo si} \quad n+q \leq p+m\,.\end{aligned}$$

Por ejemplo, $[(1,4)] \leq_{\mathbb{Z}} [(3,2)]$ porque $1+2 \leq 3+4$.

Como lo ilustra el ejemplo anterior, debemos asegurarnos de que la definición no sea ambigua. En nuestro ejemplo debemos observar que $[(1,4)] = [(13,16)]$. ¿Será cierto que $[(13,16)] \leq_{\mathbb{Z}} [(3,2)]$? Esperamos que sí, porque de otra manera, la definición estaría mal hecha. Debemos verificar que la definición de $\leq_{\mathbb{Z}}$ no depende del representante de las clases $[(n,m)]$ y $[(p,q)]$. En estricto rigor, mientras no probemos que una supuesta relación está bien definida no podemos llamarla relación. Lo mismo ocurre para funciones. A menudo se comete el abuso de lenguaje de "definir la relación R" para después demostrar que está bien definida. Esta práctica es inofensiva y la adoptaremos, por ejemplo, en el siguiente teorema.

Teorema 2.28. *La relación $\leq_{\mathbb{Z}}$ está bien definida.*

Demostración. Supongamos que $[(n,m)] = [(n',m')]$ y $[(p,q)] = [(p',q')]$, es decir, $n+m' = n'+m$ y también $p+q' = p'+q$. Suponiendo que $[(n,m)] \leq_{\mathbb{Z}} [(p,q)]$ debemos demostrar que $[(n',m')] \leq_{\mathbb{Z}} [(p',q')]$.

Tenemos entonces que $n+q \leq p+m$. Luego

$$\begin{array}{rcll}
(n+q)+(m'+q') & \leq & (p+m)+(m'+q') & \textit{sumando } m'+q', \\
(n+m')+(q+q') & \leq & (p+q')+(m+m') & \textit{asociat. y conmutat. en } \mathbb{N}, \\
(n'+m)+(q+q') & \leq & (p'+q)+(m+m') & \textit{porque } n+m' = n'+m, \\
(n'+q')+(m+q) & \leq & (p'+m')+(m+q) & \textit{asociat. y conmut. en } \mathbb{N}, \\
n'+q' & \leq & p'+m' & \textit{cancelación en } \mathbb{N},
\end{array}$$

o sea, $[(n',m')] \leq_{\mathbb{Z}} [(p',q')]$, que es lo que queríamos demostrar. □

Debemos ahora demostrar que $\leq_{\mathbb{Z}}$ es un orden.

Teorema 2.29. *La relación $\leq_{\mathbb{Z}}$ es un orden total, discreto, sin primer ni último elemento.*

Demostración. La relación $\leq_{\mathbb{Z}}$ es obviamente reflexiva.

Para verificar la antisimetría, supongamos que $[(n,m)] \leq_{\mathbb{Z}} [(p,q)]$ y $[(p,q)] \leq_{\mathbb{Z}} [(n,m)]$. Esto significa que $n+q \leq p+m$ y $p+m \leq n+q$. Entonces, por la

antisimetría del orden de los naturales, $n+q=p+m$, es decir, $(n,m)\,R\,(p,q)$, o sea, $[(n,m)]=[(p,q)]$.

Verifiquemos la transitividad. Supongamos que $[(n,m)]\leq_{\mathbb{Z}}[(p,q)]$ y $[(p,q)]\leq_{\mathbb{Z}}[(r,s)]$. Entonces $n+q\leq p+m$ y $p+s\leq r+q$.

$$\begin{array}{rcll}(n+q)+s & \leq & (p+m)+s & \textit{sumando } s \textit{ a ambos lados},\\ (n+s)+q & \leq & (p+s)+m & \textit{asociatividad y conmutatividad en } \mathbb{N},\\ (n+s)+q & \leq & (r+q)+m & p+s\leq r+q \textit{ y Teo.}2.26,2.\text{a.},\\ (n+s)+q & \leq & (r+m)+q & \textit{asociatividad y conmutatividad en } \mathbb{N},\\ n+s & \leq & r+m & \textit{cancelación en } \mathbb{N}.\end{array}$$

o sea, $[(n,m)]\leq_{\mathbb{Z}}[(r,s)]$, que es lo que queríamos demostrar.

Veremos ahora que el orden $\leq_{\mathbb{Z}}$ es un orden total. Sean $[(n,m)]$ y $[(p,q)]$ dos enteros. Entonces como $n+q$ y $p+m$ son números naturales, o bien $n+q<p+m$ o bien $n+q=p+m$ o bien $p+m<n+q$. Por lo tanto, $[(n,m)]\leq_{\mathbb{Z}}[(p,q)]$ o bien $[(n,m)]=[(p,q)]$ o bien $[(p,q)]\leq_{\mathbb{Z}}[(n,m)]$.

El orden $\leq_{\mathbb{Z}}$ es discreto porque dado cualquier entero $[(n,m)]$, su sucesor inmediato es $[(n+1,m)]$. En efecto, $[(n,m)]<_{\mathbb{Z}}[(n+1,m)]$, ya que $n+m<(n+1)+m$.

Por otra parte, si $[(n,m)]<_{\mathbb{Z}}[(p,q)]<_{\mathbb{Z}}[(n+1,m)]$, entonces

$$n+q<p+m<(n+1)+q=(n+q)+1\,,$$

y tendríamos que el número natural $p+m$ estaría entre $n+q$ y su sucesor $(n+q)+1$, lo que es una contradicción.

Por último, es claro que $\leq_{\mathbb{Z}}$ no tiene primer ni último elemento, porque dado cualquier entero $[(n,m)]$ hay uno más grande, por ejemplo $[(n+1,m)]$ y también uno más chico, por ejemplo, $[(n,m+1)]$. □

Definimos el conjunto de los *enteros positivos*

$$\mathbb{Z}^+=\{[(n,m)]\,:\,[(0,0)]<_{\mathbb{Z}}[(n,m)]\}=\{[(n,m)]\,:\,n>m\}\,.$$

Similarmente, el conjunto de los *enteros negativos*

$$\mathbb{Z}^-=\{[(n,m)]\,:\,[(n,m)]<_{\mathbb{Z}}[(0,0)]\}=\{[(n,m)]\,:\,n<m\}\,.$$

2.2.2 Operaciones con Números Enteros

Definición 2.30. La suma de dos enteros $[(n,m)]$ y $[(p,q)]$ es el entero

$$[(n,m)]\oplus[(p,q)]=[(n+p,m+q)]\,.$$

El producto o multiplicación de dos enteros $[(n,m)]$ y $[(p,q)]$ es el entero

$$[(n,m)]\odot[(p,q)]=[(np+mq,mp+nq)]\,.$$

Hemos usado los símbolos $\oplus$ y $\odot$ para representar la suma y el producto de enteros, para enfatizar que las correspondientes operaciones con números naturales son, en este contexto, cosas muy distintas. Al final de esta sección veremos que existe una correspondencia tal entre estos conjuntos y sus operaciones, que no es necesario hacer la distinción. Sin embargo, como veremos a continuación, las propiedades de las operaciones con enteros se prueban usando propiedades de las operaciones con los naturales y es mejor tener siempre claro cuál de ellas se está usando.

Teorema 2.31. *Las operaciones de suma y multiplicación de números enteros están bien definidas.*

Demostración. Debemos comprobar que dichas operaciones no dependen del representante de la clase de equivalencia que usemos.

Supongamos que $[(n,m)] = [(n',m')]$ y $[(p,q)] = [(p',q')]$, es decir, $n+m' = n'+m$ y también $p+q' = p'+q$. Entonces

$$\begin{aligned}
(n+m')+(p+q') &= (n'+m)+(p'+q) && \textit{sumando ambas identidades},\\
(n+p)+(m'+q') &= (n'+p')+(m+q) && \textit{asoc. y conmut. en } \mathbb{N},\\
(n+p,m+q)\ R\ (n'+p',m'+q') && && \textit{definición de } R,\\
[(n+p,m+q)] &= [(n'+p',m'+q')] && \textit{definición de clase},\\
[(n,m)]+[(p,q)] &= [(n',m')]+[(p',q')] && \textit{definición de suma},
\end{aligned}$$

que es lo que queríamos demostrar.

En forma similar probamos que la multiplicación está bien definida. □

El próximo teorema nos entrega las principales propiedades estructurales de la suma que convierten a los enteros en un grupo abeliano. Para más información sobre el concepto de grupo ver, por ejemplo, [**7**].

Teorema 2.32. *La suma de números enteros verifica las siguientes propiedades.*

1. *La suma de números enteros es asociativa.*
2. *La suma de números enteros es conmutativa.*
3. *El entero* $[(0,0)]$ *es neutro con respecto a la suma, es decir, para todo entero* $[(n,m)]$, $[(n,m)] \oplus [(0,0)] = [(n,m)]$.
4. *Todo entero* $x = [(n,m)]$ *tiene un inverso aditivo, es decir, un entero* y *tal que* $x \oplus y = 0$. *Este inverso es único y lo denotaremos* $\ominus x$.

Demostración.

1. Para todo n, m y p se tiene

$$\begin{aligned}
([n,m)] \oplus [p,q)]) \oplus [(r,s)] &= [(n+p,m+q)] \oplus [(r,s)] && \textit{definición de suma},\\
&= [(n+p)+r,(m+q)+s)] && \textit{definición},\\
&= [(n+(p+r),m+(q+s))] && \textit{asociatividad en } \mathbb{N},\\
&= [(n,m)] \oplus [(p+r,q+s)] && \textit{definición},\\
&= [(n,m)] \oplus ([(p,q)] \oplus [(r,s)]) && \textit{definición},
\end{aligned}$$

o sea, la suma de enteros es asociativa. Observe que la asociatividad de la suma de enteros descansa directamente en la asociatividad de la suma de los números naturales.

2. De manera análoga se demuestra que la suma de números enteros es conmutativa.

3. Para todo n y m se tiene $[n,m)] \oplus [0,0)] = [(n+0, m+0)] = [(n,m)]$, tal como se planteó.

4. Dado el entero $[(n,m)]$, consideramos $[(m,n)]$ y sumamos $[(n,m)] \oplus [(m,n)] = [(n+m, m+n)] = [(0,0)]$, o sea, $[(m,n)]$ es el inverso aditivo de $[(n,m)]$. Vemos entonces que $\ominus[(n,m)] = [(m,n)]$.

Es claro que el inverso es único. Supongamos por el contrario que $[(p,q)]$ y $[(r,s)]$ son dos inversos aditivos de $[(m,n)]$. Entonces

$$
\begin{aligned}
&[(n,m)] \oplus [(p,q)] = [(n,m)] \oplus [(r,s)] = [(0,0)] && \textit{condición dada},\\
&[(n+p, m+q)] = [(n+r, m+s)]\,, && \textit{definición de suma},
\end{aligned}
$$

o sea,

$$
\begin{aligned}
n+p = n+r \quad \text{y} \quad m+q = m+s & \\
p = r \quad \text{y} \quad q = s && \textit{por cancelación en } \mathbb{N},\\
[(p,q)] = [(r,s)] && \textit{por definición}.
\end{aligned}
$$

□

Teorema 2.33. *Los números enteros verifican la ley de cancelación para la suma, es decir, si x, y, $z \in \mathbb{Z}$ son tales que $x+z = y+z$, entonces $x = y$.*

Demostración. La ley de cancelación de la suma de números enteros se puede demostrar directamente, reduciéndola a un problema de cancelación de la suma de números naturales.

Alternativamente, se puede demostrar usando las propiedades del inverso aditivo. Supongamos que

$$
\begin{aligned}
&[(n,m)] \oplus [(r,s)] = [(p,q)] \oplus [(r,s)] & &\\
&(\,[n,m)] \oplus [(r,s)]\,) \oplus [(s,r)] = (\,[(p,q)] \oplus [(r,s)]\,) \oplus [(s,r)] && \textit{sumando } [(s,r)]\,,\\
&[n,m)] \oplus (\,[(r,s)] \oplus [(s,r)]\,) = [(p,q)] \oplus (\,[(r,s)]) \oplus [(s,r)]\,) && \textit{asociatividad},\\
&[(n,m)] \oplus [(0,0)] = [(p,q)] \oplus [(0,0)] && \textit{por } 4,\\
&[(n,m)] = [(p,q)] && \textit{por } 3.
\end{aligned}
$$

□

El siguiente teorema reúne las principales propiedades estructurales del producto de enteros, las que junto a las de la suma que aparecen en el Teorema 2.32 convierten a los enteros en un anillo conmutativo y unitario.

Teorema 2.34. *El producto de números enteros verifica las siguientes propiedades.*

1. *El producto de números enteros es asociativo.*
2. *El producto de números enteros es conmutativo.*
3. *El entero $[(1,0)]$ es neutro con respecto a la multiplicación, es decir, para todo entero $[(n,m)]$, se tiene $[(n,m)] \odot [(1,0)] = [(n,m)]$.*
4. *El producto de números enteros es distributivo sobre la suma.*

Demostración. Las propiedades 1, 2 y 4 se reducen en forma inmediata a las mismas propiedades de los números naturales en cada una de las coordenadas.

La propiedad 3 es inmediata aplicando la definición de producto. □

Teorema 2.35. *El producto de números enteros verifica las siguientes propiedades.*

1. *Para todo entero* x, $x \odot [(0,0)] = [(0,0)]$.
2. *En los números enteros no hay divisores del cero, es decir, si* x *e* y *son dos enteros tales que* $x \odot y = [(0,0)]$, *entonces o bien* $x = [(0,0)]$ *o bien* $y = [(0,0)]$.
3. *Vale la ley de cancelación para la multiplicación por un entero distinto de cero, es decir, si* $x, y, z \in \mathbb{Z}$, $z \neq [(0,0)]$ *y* $x \odot z = y \odot z$, *entonces* $x = y$.
4. *Si* $x, y \in \mathbb{Z}$, *entonces* $(\ominus x) \odot (\ominus y) = x \odot y$.

Demostración.

1. Sea $[(m,n)]$ un número entero. Se tiene

$$[(n,m)] \odot [(0,0)] = [(n\,0 + m\,0, m\,0 + n\,0)] = [(0,0)]\,.$$

2. Supongamos que $[(n,m)] \odot [(p,q)] = [(0,0)]$ y que $[(n,m)] \neq [(0,0)]$, es decir $n \neq m$, digamos sin perdida de generalidad, que $n > m$. Recordemos que en tal caso existe un único número natural d tal que $n = m+d$, en este caso $d \neq 0$. La condición dada es $[(np+mq, mp+nq)] = [(0,0)]$, o lo que es lo mismo, $np + mq = mp + nq$, entonces

$$\begin{array}{rcll}
np + mq & = & mp + nq & \\
(m+d)p + mq & = & mp + (m+d)q & \textit{porque } n = m + d, \\
(mp + dp) + mq & = & mp + (mq + dq) & \textit{distributividad en } \mathbb{N}, \\
mp + (dp + mq) & = & mp + (mq + dq) & \textit{asociatividad en } \mathbb{N}, \\
dp + mq & = & mq + dq & \textit{cancelación en } \mathbb{N}, \\
dp + mq & = & dq + mq & \textit{conmutatividad en } \mathbb{N}, \\
dp & = & dq & \textit{cancelación de suma en } \mathbb{N}, \\
p & = & q & d \neq 0 \textit{ y cancelación de producto en } \mathbb{N},
\end{array}$$

o sea, $[(p,q)] = [(0,0)]$, que es lo que queríamos demostrar. Observemos que una vez más, la propiedad es demostrada usando la correspondiente propiedad de los números naturales.

3. Supongamos que $[(x,y)] \neq [(0,0)]$ y que $[(n,m)] \odot [(x,y)] = [(p,q)] \odot [(x,y)]$. Ahora sumemos $[(q,p)] \odot [(x,y)]$ a ambos lados. Tenemos:

$$\begin{array}{ll}
[(n,m)] \odot [(x,y)] + [(q,p)] \odot [(x,y)] = [(p,q)] \odot [(x,y)] + [(q,p)] \odot [(x,y)] & \\
([(n,m)] + [(q,p)]) \odot [(x,y)] = ([(p,q)] + [(q,p)]) \odot [(x,y)] & \textit{distributividad en } \mathbb{Z}, \\
[(n+q, m+p)] \odot [(x,y)] = [(p+q, q+p)] \odot [(x,y)] & \textit{sumando}, \\
[(n+q, m+p)] \odot [(x,y)] = [(0,0)] \odot [(x,y)] & \\
[(n+q, m+p)] \odot [(x,y)] = [(0,0)] & 1.
\end{array}$$

Por 2, $[(n+q, m+p)] = [(0,0)]$, es decir, $n+q = p+m$, o sea, $[(n,m)] = [(p,q)]$, que es lo que queríamos demostrar.

4. Sean $[(n,m)]$ y $[(p,q)]$ dos enteros. Entonces

$$(-[(n,m)])\odot(-[(p,q)]) = [(m,n)])\odot[(q,p)] = [(mq+np, mp+nq)] = [(n,m)])\odot[(p,q)]\,.$$

□

El último punto del teorema anterior, implica una característica de la multiplicación de números enteros que a menudo resulta difícil de explicar, a saber, que el producto de dos números negativos sea positivo. Es común que los profesores ideen ingeniosas explicaciones que involucran amigos, enemigos, amigos de los amigos, etc. para tratar de justificar esta aparente anomalía. Como vimos anteriormente, en nuestro modelo conjuntista de los números enteros, la propiedad se deriva fácilmente de las definiciones. Sin embargo, esta simplicidad oculta lo que realmente sucede. En la práctica, sólo nos dice que nuestro modelo es correcto e incluso elegante, pero se corre el peligro de pensar que el producto de enteros negativos es positivo *porque* así ocurre con estos conjuntos. La verdad, es que ello es sólo el resultado necesario de requerir que las operaciones con números negativos tengan las mismas propiedades algebraicas que las operaciones con números positivos, asociatividad, conmutatividad, distributividad, etc.

2.2.3 Los Enteros y los Naturales

Estamos acostumbrados a considerar que los números naturales están contenidos en los enteros, coincidiendo con los enteros positivos y el cero. Es claro que en esta construcción esto no sucede. Sería difícil confundir el natural 1 con el entero que hace el papel de 1 en $\mathbb{Z}$, a saber, $[(1,0)] = \{(n+1,1) \,:\, n \in \mathbb{N}\}$. Como conjuntos son totalmente distintos, mientras el primero tiene un solo elemento, el segundo es infinito. Sin embargo, esta relación intuitiva entre números naturales y enteros se refleja en nuestro modelo conjuntista de una manera muy sencilla.

Estudiemos un poco la estructura de cada uno de los conjuntos $[(n,m)]$ a los que hemos llamado número entero. Si $n \geq m$, existe un par de la forma $(r,0)$ tal que $(r,0) \in [(n,m)]_R$. A su vez, si $n < m$, existe un par de la forma $(0,r)$ tal que $(0,r) \in [(n,m)]_R$. En cada caso, estos números naturales r son obviamente únicos. Es habitual elegir como representante de cada clase a este elemento distinguido.

Existe una obvia inyección de $\mathbb{N}$ en $\mathbb{Z}$, a saber

$$\begin{aligned} F \,:\, \mathbb{N} &\longrightarrow \mathbb{Z} \\ n &\longmapsto [(n,0)]. \end{aligned}$$

El conjunto $F[\mathbb{N}] = \{[(n,0)] \,:\, n \in \mathbb{N}\} \subseteq \mathbb{Z}$ es una especie de copia de los naturales dentro de los enteros que se comporta exactamente igual a los naturales, de

manera que, abusando del lenguaje, podemos decir que los naturales coinciden con los enteros positivos unidos al cero y denotar a los enteros como sigue:

$$[(n,m)] = \begin{cases} r & , \text{ si } (r,0) \in [(n,m)] \\ 0 & , \text{ si } n = m \\ -r & , \text{ si } (0,r) \in [(n,m)] \end{cases},$$

Por ejemplo, $-5 = \{(0,5),(1,6),(2,7),(3,8),\cdots\}$ y $5 = \{(5,0),(6,1),(7,2),\cdots\}$. Observe que $0 = [(n,n)] = \ominus 0$.

Comprobemos ahora que la copia de los naturales dentro de los enteros se comporta como los naturales.

Teorema 2.36. *Sean n, m y $r \in \mathbb{N}$.*

1. $[(n,0)] \leq_{\mathbb{Z}} [(m,0)]$ *si y solo si* $n < m$
2. $[(n,0)] \oplus [(m,0)] = [(r,0)]$ *si y solo si* $n + m = r$
3. $[(n,0)] \odot [(m,0)] = [(r,0)]$ *si y solo si* $n\,m = r$.

Demostración. Esto resulta directamente de las definiciones de orden y de las operaciones en los enteros. □

Este teorema implica que los enteros positivos unidos al cero se comportan igual que los números naturales, por lo tanto, si bien en el modelo conjuntista el número natural n y el número entero n son objetos muy distintos, esta distinción es inofensiva y para todo efecto práctico, es decir, su uso en la construcción de la matemática dentro de la teoría de conjuntos, son indistinguibles.

De ahora en adelante podemos olvidarnos de las clases de equivalencia y usar esta conveniente notación. Podemos también dejar de usar símbolos especiales para las operaciones $\oplus$ y $\odot$ reemplazándolas por las habituales $+$ y $\cdot$, para suma y multiplicación, respectivamente.

2.2.4 Ejercicios

1. Dé los detalles que no se hicieron en la demostración del Teorema 2.32.
2. Demuestre todas las afirmaciones que no se demostraron en el Teorema 2.34.
3. Dé los detalles de la demostración del Teorema 2.36.
4. Demuestre que el cuadrado de todo número entero es positivo.

2.3 Los Números Racionales

La construcción de los números racionales se hace en forma similar a la construcción de los enteros, como clases de equivalencia de pares de números enteros. Sin embargo, esta vez la relación de equivalencia es mucho más natural e intuitiva, ya que refleja una característica de las fracciones que hemos utilizado desde la escuela básica, a saber, que las fracciones se pueden amplificar y simplificar sin variar su valor.

Sea R la relación definida sobre $\mathbb{Z}\times(\mathbb{Z}-\{0\})$, el conjunto de los pares ordenados de números enteros tales que el segundo es distinto de 0, definida por

$$(n,m)\,R\,(p,q) \quad \text{ si y solo si } \quad n\,q = p\,m\,.$$

Teorema 2.37. *R es una relación de equivalencia.*

Demostración. Como $n\,m = n\,m$, se tiene $(n,m)\,R\,(n,m)$, o sea, R es reflexiva.

Por definición R es obviamente simétrica.

Para verificar la transitividad, supongamos que $(n,m)\,R\,(p,q)$ y que $(p,q)\,R\,(r,s)$. Entonces $n\,q = p\,m$ y $p\,s = r\,q$.

$$\begin{aligned}
(nq)(rs) &= (pm)(rs) && \text{multiplicando la primera ecuación por } r\,s\,,\\
n(q(rs)\,) &= p\,(m(rs)\,) && \text{asociatividad en } \mathbb{Z},\\
n(\,(qr)s) &= p\,(\,(mr)s) && \text{asociatividad en } \mathbb{Z},\\
n(s(qr)\,) &= (p\,(mr)\,)\,s && \text{conmutatividad y asociatividad en } \mathbb{Z},\\
(ns)(qr) &= (\,(mr)p)\,s && \text{asociatividad y conmutatividad en } \mathbb{Z}\\
(ns)(rq) &= (mr)(ps) && \text{asociatividad en } \mathbb{Z},\\
(ns)(rq) &= (mr)(rq) && p\,s = r\,q,
\end{aligned}$$

pero $ps = rq \neq 0$, luego por el Teorema 2.35 3, podemos cancelar en la última línea obteniendo $n\,s = r\,m$, o sea, $(m,n)\,R\,(r,s)$, que es lo que queríamos demostrar. □

Si denotamos $[(n,m)]_R$ a la clase de equivalencia del par (n,m), definimos el conjunto $\mathbb{Q}$ de los *números racionales*

$$\mathbb{Q} = \{\,[(n,m)]_R \;:\; n,m\in\mathbb{Z},\; m\neq 0\}\,.$$

Para no hacer la lectura tan complicada simplificaremos la notación eliminando el subíndice R de modo que $[(n,m)]_R$ en adelante se escribirá $[(n,m)]$.

Observemos también que si c es cualquier entero distinto de 0, entonces $[(n,m)] = [(n\,c, m\,c)]$. Esta propiedad corresponde a la amplificación de una fracción, o sea, multiplicar numerador y denominador por un mismo número. Una consecuencia de la amplificación es que en cada clase hay algún representante cuya segunda componente, que intuitivamente corresponde al denominador de la fracción correspondiente, es positivo. Si m es negativo, basta tomar $c = -1$.

Intuitivamente el racional $[(n,m)]$ corresponde a la fracción $\frac{n}{m}$ y muchos libros usan este último símbolo, la fracción, para denotar la clase, es decir, al número racional. En este contexto entonces la fracción $\frac{1}{2}$ corresponde a la clase $[(1,2)]$. Por lo tanto,

$$\frac{1}{2} = [(1,2)] = [(2,4)] = \frac{2}{4}\,.$$

El manejo inadecuado del concepto de clase de equivalencia suele traer aparejada una confusión en este punto. Algunos opinan que el racional $\frac{1}{2}$ y el racional $\frac{2}{4}$ son *equivalentes, pero no iguales*. Lo cierto es que ambas fracciones representan a la misma clase de equivalencia, de tal manera que si son denotadas por las fracciones $\frac{1}{2}$ y $\frac{2}{4}$,

estas son iguales. Por otra parte, los representantes escogidos $(1,2)$ y $(2,4)$, (u otros), son equivalentes, pero no iguales. Esto es similar a lo que ocurre con los numeros naturales $1+1$ y $4-2$ ambas expresiones representan al número dos y, por lo tanto, son iguales entre sí.

La construcción que acabamos de hacer es un caso particular de algo muy general, llamado la construcción del cuerpo de cuocientes de un dominio de integridad. Este es el cuerpo más pequeño que contiene al dominio. En un contexto algebraico general, entonces, los números racionales son el cuerpo de cuocientes del dominio de los números enteros. Otro ejemplo interesante es el cuerpo de cuocientes del dominio de los polinomios con coeficientes reales, constituido por las funciones racionales, es decir, funciones que son cuocientes de polinomios. Para más información sobre dominios, cuerpos y otros conceptos algebraicos ver, por ejemplo, [**6**].

2.3.1 Orden

Cuando pensamos en el orden de los números racionales la primera idea es seguir nuestra intuición y decir que

$$\frac{n}{m} \text{ es menor que } \frac{p}{q} \quad \text{si y solo si} \quad n\,q <_{\mathbb{Z}} p\,m\,.$$

Esta intuición es correcta sólo si ambos denominadores son positivos o ambos son negativos, pero si no lo son el orden se invierte. Por ejemplo, sabemos que

$$\frac{1}{3} \text{ es menor que } \frac{-1}{-2}\,, \quad \text{pero} \quad 1\,(-2) \not<_{\mathbb{Z}} (-1)\,3\,.$$

Existe, sin embargo, una manera ingeniosa de lograr que ambos denominadores sean positivos usando otro representante de la clase. En efecto, hemos visto que

$$\frac{n}{m} = \frac{n\,m}{m\,m} \quad \text{y} \quad \frac{p}{q} = \frac{p\,q}{q\,q}\,,$$

y ahora los denominadores de las segundas fracciones son enteros positivos porque son cuadrados.

Usando esta observación y recordando que no debería importar qué representante de la clase usemos, los números racionales pueden ser ordenados de la siguiente manera.

$$[(n,m)] <_{\mathbb{Q}} [(p,q)] \quad \text{si y solo si} \quad (n\,m)\,(q\,q) <_{\mathbb{Z}} (p\,q)\,(m\,m)\,.$$

Obsérvese que la primera relación, $<_{\mathbb{Q}}$, es entre números racionales y la segunda, $<_{\mathbb{Z}}$, es entre números enteros. Usaremos también la notación

$$\begin{aligned} [(n,m)] \leq_{\mathbb{Q}} [(p,q)] \quad &\text{si y solo si} \quad [(n,m)] <_{\mathbb{Q}} [(p,q)] \quad \text{ó} \quad [(n,m)] = [(p,q)] \\ &\text{si y solo si} \quad (n,m)\,(q\,q) \leq_{\mathbb{Z}} (p\,q)\,(m\,m)\,. \end{aligned}$$

Por ejemplo, $[(1,4)] \leq_{\mathbb{Q}} [(3,2)]$ porque $8 = 1\cdot 4\cdot 2\cdot 2 \leq_{\mathbb{Z}} 3\cdot 2\cdot 4\cdot 4 = 96$ y también $[(2,-4)] \leq_{\mathbb{Q}} [(1,3)]$ porque $-72 = 2\cdot(-4)\cdot 3\cdot 3 \leq_{\mathbb{Z}} 1\cdot 3\cdot(-4)\cdot(-4) = 48$.

Al igual que en el caso de los enteros, debemos demostrar que esta definición no depende de los representantes empleados.

Teorema 2.38. *La relación $\leq_{\mathbb{Q}}$ está bien definida.*

Demostración. La demostración es similar a la del Teorema 2.28 cambiando sumas por productos.

Consideremos cuatro racionales tales que $[(n,m)] = [(n',m')]$ y $[(p,q)] = [(p',q')]$, es decir, $n\,m' = n'\,m$ y también $p\,q' = p'\,q$. Suponiendo que $[(n,m)] \leq_{\mathbb{Z}} [(p,q)]$ debemos demostrar que $[(n',m')] \leq_{\mathbb{Z}} [(p',q')]$.

Tenemos entonces

$$\begin{array}{rcll}
(n\,m)(q\,q) & \leq_{\mathbb{Z}} & (p\,q)(m\,m) & \textit{definición de } \leq_{\mathbb{Q}}, \\
(n\,m)(q\,q)(m'\,m')(q'\,q') & \leq_{\mathbb{Z}} & (p\,q)(m\,m)(m'\,m')(q'\,q') & \textit{multipl. } (m'\,m')(q'\,q'), \\
(n\,m')(m\,m')(q'\,q')(q\,q) & \leq_{\mathbb{Z}} & (p\,q')(q\,q')(m'\,m')(m\,m) & \textit{asoc. y conmut. en } \mathbb{Z}, \\
(n'\,m)(m\,m')(q'\,q')(q\,q) & \leq_{\mathbb{Z}} & (p'\,q)(q\,q')(m'\,m')(m\,m) & n\,m' = n'\,m\ ;\ p\,q' = p'\,q, \\
n'\,(m\,m)\,m'(q'\,q')(q\,q) & \leq_{\mathbb{Z}} & p'\,(q\,q)\,q'(m'\,m')(m\,m) & \textit{asociatividad en } \mathbb{Z}, \\
(n'\,m')(q'\,q') & \leq_{\mathbb{Z}} & (p'\,q')(m'\,m') & \textit{cancelando } (m\,m)\,(q\,q),
\end{array}$$

o sea, $[(n',m')] \leq_{\mathbb{Q}} [(p',q')]$, que es lo que queríamos demostrar. □

La definición anterior es bastante complicada y hay otra más sencilla. Definimos el orden por casos:

$$[(n,m)] \leq_{\mathbb{Q}} [(p,q)] \quad \text{sii} \quad \begin{cases} n\,q \leq_{\mathbb{Z}} p\,m & \text{si } m \text{ y } q \text{ son del mismo signo}, \\ n\,q \geq_{\mathbb{Z}} p\,m & \text{si no.} \end{cases}$$

La aparente mayor simplicidad de esta definición tiene un precio. Las demostraciones son mucho más complejas porque hay que demostrar todas las combinaciones de casos posibles. Es por esto, además de ser más compacta y elegante, que hemos preferido la definición dada.

Debemos ahora demostrar que $\leq_{\mathbb{Q}}$ es un orden y que tiene ciertas propiedades. La más importante es que se trata de un *orden denso*, esto es, dados dos números racionales a y b, tales que $a < b$, existe un racional c tal que $a < c < b$.

Teorema 2.39. *La relación $\leq_{\mathbb{Q}}$ es un orden total, denso, sin primer ni último elemento.*

Demostración. La demostración de que $\leq_{\mathbb{Q}}$ es un orden total es similar a la del Teorema 2.29 cambiando adecuadamente las operaciones y usando las propiedades respectivas del orden de los enteros.

El orden $\leq_{\mathbb{Q}}$ es denso porque dados cualesquiera dos racionales $[(n,m)] <_{\mathbb{Q}} [(p,q)]$ podemos intercalar un racional entre ellos. En efecto, abreviando como es usual $x\,x = x^2$,

$$\begin{array}{rcll}
(n\,m)q^2 & <_{\mathbb{Z}} & (p\,q)m^2 & \textit{definición}, \\
2(n\,m)q^2m^2 & <_{\mathbb{Z}} & 2(p\,q)m^2m^2 & \textit{multiplicando } 2m^2, \\
4(n\,m)q^2m^2 & <_{\mathbb{Z}} & 2(p\,q)m^2m^2 + 2(n\,m)q^2m^2 & \textit{sumando } 2(n\,m)q^2m^2, \\
(n\,m)(2q\,m)^2 & <_{\mathbb{Z}} & (p\,m + n\,q)(2q\,m)m^2 & \textit{asoc. y conm. en } \mathbb{Z},
\end{array}$$

es decir, $[(n,m)] <_{\mathbb{Q}} [(p\,m + n\,q, 2qm)]$.

De manera análoga probamos que $[(n\,q + p\,m\,, 2\,q\,m)] <_{\mathbb{Q}} [(p,q)]$, probando que el racional $[(n\,q + p\,m\,, 2\,q\,m)]$ está entre $[(n,m)]$ y $[(p,q)]$, por lo tanto, $\leq_{\mathbb{Q}}$ es un orden denso.

Por último, es claro que $\leq_{\mathbb{Q}}$ no tiene primer ni último elemento porque dado cualquier racional $[(n,m)]$, con $0 <_{\mathbb{Z}} m$, hay un racional más grande, por ejemplo, $[(n+1,m)]$ y también uno más chico, por ejemplo, $[(n-1,m)]$. □

2.3.2 Operaciones con los Números Racionales

Definición 2.40. La suma de dos racionales $[(n,m)]$ y $[(p,q)]$ es el entero

$$[(n,m)] \oplus [(p,q)] = [(nq + mp, mq)]\,.$$

El producto o multiplicación de dos racionales $[(n,m)]$ y $[(p,q)]$ es el número racional

$$[(n,m)] \odot [(p,q)] = [(np, mq)]\,.$$

Nuevamente hemos usado los símbolos $\oplus$ y $\odot$ para representar la suma y el producto de racionales dejando los símbolos corrientes $+$ y $\cdot$ para las correspondientes operaciones con números enteros. Más adelante en esta sección, veremos que, como antes hicimos con naturales y enteros, existe una inyección de los enteros en los racionales que hace innecesario hacer la distinción. Sin embargo, como en el caso anterior, las propiedades de las operaciones con racionales se prueban usando propiedades de las operaciones con los enteros y es mejor tener siempre claro cuál operación se está usando.

Teorema 2.41. *Las operaciones de suma y multiplicación de números racionales están bien definidas.*

Demostración. Supongamos que $[(n,m)] = [(n',m')]$ y $[(p,q)] = [(p',q')]$. Entonces

$$\begin{array}{rcll}
n\,m' & = & n'\,m \quad (*) & \textit{definición de } R,\\
p\,q' & = & p'\,q \quad (**) & \textit{definición de } R,\\
(nm')(qq') & = & (n'm)(qq') & \textit{multiplicando } (*) \textit{ por } q\,q',\\
(mm')(pq') & = & (mm')(p'q) & \textit{multiplicando } (**) \textit{ por } m\,m',\\
(nm'qq') + (mm'pq') & = & (mm'p'q) + (n'mqq') & \textit{sumando},\\
(nq+mp)m'q' & = & (m'p' + n'q')mq & \textit{factorizando},\\
(nq+mp, mq) & R & (n'q' + m'p', m'q') & \textit{definición de } R,\\
[(nq+mp, mq)] & = & [(n'q' + m'p', m'q')] & \textit{definición de clase},\\
[(n,m)] \oplus [(p,q)] & = & [(n',m')] \oplus [(p',q')] & \textit{definición de suma},
\end{array}$$

que es lo que queríamos demostrar.

En forma similar probamos que la multiplicación está bien definida.

$$\begin{array}{rcll}
(nm')(pq') & = & (n'm)(pq') & \textit{multiplicando } (*) \textit{ por } pq' \\
(np)(m'q') & = & (n'p)(mq') & \textit{reordenando en } \mathbb{Z} \\
(pq')(n'm) & = & (p'q)(n'm) & \textit{multiplicando } (**) \textit{ por } n'm, \\
(n'p)(mq') & = & (n'p')(mq) & \textit{reordenando en } \mathbb{Z} \\
(np)(m'q') & = & (n'p')(mq) & \textit{igualando términos,} \\
(np, mq) & R & (n'p', m'q') & \textit{definición de } R, \\
[(np, mq)] & = & [(n'p', m'q')] & \textit{definición de clase,} \\
[(n, m)] \odot [(p, q)] & = & [(n', m')] \odot [(p', q')] & \textit{definición de producto,}
\end{array}$$

que es lo que queríamos demostrar. □

Ejemplo 2.42. Podemos ahora ver que no existe un racional r tal que $r^2 = 2$, en otras palabras, ningún número racional es la raíz cuadrada de 2. En la próxima sección construiremos un número real que corresponde a dicha raíz. Sea $[(n, m)]$ un racional. Podemos escoger, por sucesivas simplificaciones, un representante tal que n y m no tienen divisores comunes. Si suponemos que $[(n, m)]^2 = [(n^2, m^2)] = [(2, 1)]$, entonces $n^2 = 2m^2$, o sea, n^2 es par. Esto implica que n es par, digamos que $n = 2k$. Pero entonces $2m^2 = n^2 = (2k)^2 = 4k^2$. Es decir, $m^2 = 2k^2$, y, por lo tanto, m también es par. Entonces tanto m como n son pares, o sea, tienen a 2 como divisor común, contrario a nuestra suposición inicial.

Esta demostración se puede replicar para demostrar que $\sqrt{p}$ no es racional para un número entero primo p. También para demostrar que $\sqrt[3]{2}$ y, en general, $\sqrt[n]{p}$, para p primo no son números racionales, o más precisamente en el contexto de esta sección, no existe en $\mathbb{Q}$ un elemento que elevado a la n–ésima potencia es igual a p. La demostración puede adaptarse para números enteros que no son primos, pero que no son cuadrados o potencias de otro número.

Teorema 2.43. *La suma de números racionales verifica las siguientes propiedades.*

1. *La suma de números racionales es asociativa.*
2. *La suma de números racionales es conmutativa.*
3. *El racional* $\mathbf{0} = [(0, 1)]$ *es neutro con respecto a la suma, es decir, para todo racional* $[(n, m)]$, $[(n, m)] \oplus [(0, 1)] = [(n, m)]$.
4. *Todo racional* $x = [(n, m)]$ *tiene un inverso aditivo, es decir, un racional* y *tal que* $x \oplus y = \mathbf{0}$. *Este inverso es único y lo denotaremos* $\ominus x$.
5. *Vale la ley de cancelación para la suma, es decir, si* x, y, $z \in \mathbb{Q}$ *son tales que* $x \oplus z = y \oplus z$, *entonces* $x = y$.

Demostración.

1.

$$\begin{array}{rcll}
([n, m)] \oplus [p, q)]) \oplus [(r, s)] & = & [(nq + pm, mq)] \oplus [(r, s)] & \textit{def. de suma,} \\
& = & [((nq + pm)s + rmq, (mq)s)] & \textit{definición,} \\
& = & [((nqs + pms) + rmq, (mq)s)] & \textit{distrib. en } \mathbb{Z}, \\
& = & [(nqs + (ps + rq)m, m(qs))] & \textit{asociat. en } \mathbb{Z} \\
& = & [(n, m)] \oplus [(ps + rq, qs)] & \textit{definición,} \\
& = & [n, m)] \oplus ([p, q)] \oplus [(r, s)]) & \textit{definición,}
\end{array}$$

o sea, la suma de racionales es asociativa. Observe que la asociatividad de la suma de racionales descansa directamente en la asociatividad de la suma de los números enteros.

2. De manera totalmente análoga se demuestra que la suma de números racionales es conmutativa.

3. $[(n,m)] \oplus [(0,1)] = [(n\,1 + 0\,m, m\,1)] = [(n,m)]$, tal como se planteó.

4. Dado el racional $[(n,m)]$, consideremos el racional $[(-n,m)]$ y sumemos, se tiene

$$[(n,m)] \oplus [(-n,m)] = [(nm + (-n)m, m^2)] = [(0,m^2)] = [(0,1)]\,,$$

o sea, $[(-n,m)]$ es el inverso aditivo de $[(n,m)]$. Vemos entonces que $\ominus[(n,m)] = [(-n,m)]$.

Es claro que el inverso es único.

5. La ley de cancelación de la suma de números racionales se puede demostrar directamente, reduciéndola a un problema de cancelación de la suma de números enteros. □

Teorema 2.44. *El producto de números racionales verifica las siguientes propiedades.*

1. *El producto de números racionales es asociativo.*
2. *El producto de números racionales es conmutativo.*
3. *El racional* $\mathbf{1} = [(1,1)]$ *es neutro con respecto a la multiplicación, es decir, para todo racional* $[(n,m)]$, $[(n,m)] \odot [(1,1)] = [(n,m)]$.
4. *Para todo racional* $x = [(n,m)] \neq [(0,0)]$, *existe un único racional* $y = [(m,n)]$ *tal que* $x \odot y = \mathbf{1}$. *Este número se llama* inverso multiplicativo *de* x *y habitualmente se denota* $\frac{1}{x}$.
5. *El producto de números racionales es distributivo sobre la suma.*

Demostración.

3. Sea $[(m,n)]$ un número racional. Entonces $[(n,m)] \odot [(1,1)] = [(n \cdot 1, m \cdot 1)] = [(n,m)]$.

4. Dado $x = [(n,m)] \neq [(0,0)]$, tenemos que $n \neq 0$, luego $[(m,n)]$ es un racional. Además $x \odot y = [(n,m)] \odot [(m,n)] = [(nm,mn)] = [(1,1)] = \mathbf{1}$. Es claro que éste es único. □

Las propiedades descritas en el teorema anterior, junto con las correspondientes a la suma del Teorema 2.43 (excepto 5, la ley de cancelación), constituyen los axiomas que definen la estructura algebraica de cuerpo. Ver, por ejemplo, [**6**]. El siguiente teorema resume algunas de las conocidas propiedades algebraicas de los racionales.

Teorema 2.45. *El producto de números racionales verifica las siguientes propiedades.*

1. *Para todo racional* x, $x \odot \mathbf{0} = \mathbf{0}$.
2. *Vale la ley de cancelación para la multiplicación por un racional distinto de cero, es decir, si* $x, y, z \in \mathbb{Q}$, $z \neq \mathbf{0}$ *y* $x \odot z = y \odot z$, *entonces* $x = y$.

3. *En los números racionales no hay divisores del cero, es decir, si x, y son dos racionales tales que $x \odot y = \mathbf{0}$, entonces o bien $x = \mathbf{0}$ o bien $y = \mathbf{0}$.*
4. *Si x, $y \in \mathbb{Q}$, $(\ominus x) \odot (\ominus y) = x \odot y$.*

Demostración.
1. Sea $[(m,n)]$ un número racional. Entonces $[(n,m)] \odot [(0,1)] = [(n\,0, m\,1)] = [(0,m)] = [(0,1)]$.

2. Si $[(n,m)] \odot x = [(p,q)]$, donde $[(n,m)] \neq [(0,0)]$, multiplicamos ambos lados de la identidad por el inverso multiplicativo de $[(n,m)]$ obteniendo $[(m,n)] \odot ([(n,m)] \odot x) = [(m,n)] \odot [(p,q)]$. Por asociatividad, $([(m,n)] \odot ([(n,m)]) \odot x = [(mn,nm)] \odot x = [(1,1)] \odot x = x = [(mp,nq)]$.

3. Supongamos que $[(n,m)] \odot [(p,q)] = [(0,1)]$ y que $[(n,m)] \neq [(0,1)]$, es decir, $n \neq 0$. Entonces $np = 0$ y por cancelación en $\mathbb{Z}$, $p = 0$, o sea, $[(p,q)] = [(0,1)] = \mathbf{0}$.

Observemos que una vez más, la propiedad es demostrada usando propiedades de los números enteros.

4. Sean $x = [(n,m)]$ e $y = [(p,q)]$ dos racionales. Entonces

$$\begin{aligned}(\ominus x) \odot (\ominus y) = (-[(n,m)]) \odot (-[(p,q)]) &= [(-n,m)]) \odot [(-p,q)] \\ &= [((-n)(-p), mq)] \\ &= [(np, mq)] \\ &= [(n,m)]) \odot [(p,q)] = x \odot y\,.\end{aligned}$$

□

2.3.3 Los Racionales y los Enteros

Así como los números naturales están contenidos en los enteros, coincidiendo con los enteros positivos y el cero, podemos incluir en forma natural los enteros en los racionales. La idea intuitiva es obvia y la conocemos desde la enseñanza básica: los enteros son aquellos racionales cuyo denominador es 1.

Nuevamente, es claro que en esta construcción esto no es exactamente así, sin embargo, existe una obvia inyección de $\mathbb{Z}$ en $\mathbb{Q}$, a saber

$$\begin{aligned} F \;:\; \mathbb{Z} &\longrightarrow \mathbb{Q} \\ n &\longmapsto [(n,1)] \end{aligned}$$

El conjunto $\{[(n,1)] : n \in \mathbb{Z}\} \subseteq \mathbb{Q}$ es una copia de los enteros dentro de los racionales, que se comporta exactamente igual que los enteros, de manera que, abusando del lenguaje, podemos decir que los enteros coinciden con los racionales cuyo denominador es 1. Observe que $0 = [(0,1)]$ y que $1 = [(1,1)]$.

Comprobemos ahora que la copia de los enteros dentro de los racionales se comporta como los enteros.

Teorema 2.46. *Sean n, m y $r \in \mathbb{Z}$.*

1. $[(n,1)] \leq_{\mathbb{Q}} [(m,1)]$ *si y solo si* $n \leq_{\mathbb{Z}} m$
2. $[(n,1)] \oplus [(m,1)] = [(r,1)]$ *si y solo si* $n+m=r$
3. $[(n,1)] \odot [(m,1)] = [(r,1)]$ *si y solo si* $n\,m=r$.

Demostración. Esto se deriva directamente de las definiciones de orden y de las operaciones en los racionales. □

Podemos dejar de usar símbolos especiales para las operaciones $\oplus$ y $\odot$ reemplazándolas por las habituales $+$ y $\cdot$, para suma y multiplicación, respectivamente ya que la posibilidad de confusión es remota.

2.3.4 Los Racionales y la recta

Para continuar con la construcción de los números dentro de la teoría de conjuntos, veremos algunas intuiciones básicas acerca de la representación de los números en la recta numérica. Naturalmente nada de esto sucede dentro de la teoría, es sólo una intuición que nos puede ser útil, particularmente en la próxima sección, cuando construyamos los números reales. Como sabemos, hay una forma estándar de poner los números naturales en correspondencia con los puntos de una recta. Ésta es como sigue. Fijamos un punto $\mathcal{O}$ sobre una recta y a partir de él, con una cierta unidad de medida fija d, dibujamos los puntos $P_1, P_2, P_3, \ldots$ a distancias d, $2d$, $3d$, etc., hacia, digamos, la derecha de $\mathcal{O}$, tenemos una suerte de copia de los números enteros positivos y el cero sobre esa recta. Si hacemos lo mismo en la dirección opuesta y llamamos $P_{-1}, P_{-2}, P_{-3} \ldots$ etc., a los puntos obtenidos, tendremos una copia de todo $\mathbb{Z}$ en la recta. Obviamente esta copia respeta el orden, el número mayor está a la derecha del menor. También es conocido cómo funciona la suma de números enteros para esta representación en la recta.

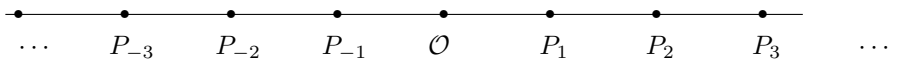


Diagrama 2

Haremos ahora la construcción de los racionales sobre la recta usando el Teorema de Thales. Consideraremos sólo números positivos construidos hacia la derecha de $\mathcal{O}$. Para los negativos podemos repetir la construcción en el sentido contrario.

Si $r = \frac{p}{q}$ es un racional, construimos dos rectas concurrentes en $\mathcal{O}$ y dibujamos un punto a distancia p de $\mathcal{O}$ sobre, digamos, la recta horizontal. De la misma manera, dibujamos puntos a distancia 1 y a distancia q de $\mathcal{O}$ sobre la otra recta. Ver el Diagrama 3. Luego unimos los puntos "p" y "q"y trazamos una paralela a esta recta pasando por "1". Esta última corta a la recta horizontal en "x". El Teorema de Thales nos dice que $x = r$.

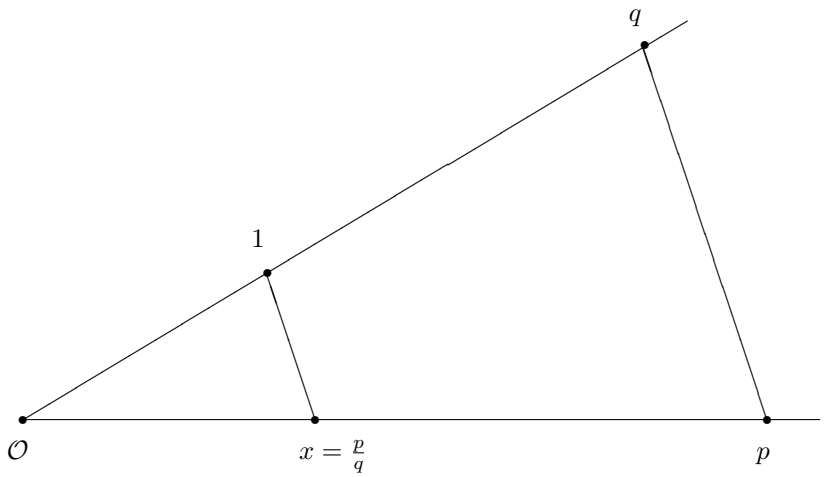


Diagrama 3

Observemos además que todas estas construcciones pueden hacerse de la manera clásica, usando sólo regla y compás.

2.3.5 Ejercicios

1. Proporcione los detalles que no se hicieron en la demostración del Teorema 2.38.
2. Proporcione los detalles que no se hicieron en la demostración del Teorema 2.44.
3. Demuestre todas las afirmaciones que no se demostraron en el Teorema 2.45.
4. Proporcione los detalles de la demostración del Teorema 2.46.
5. Demuestre que no existen números racionales r que verifiquen:
   a) $r^2 = 3$.
   b) $r^2 = 12$.
   c) $r^3 = 2$.
   d) $r^p = 2$, para algún p número natural.

2.4 Los Números Reales

Hemos visto que los números racionales se extienden a lo largo de toda la recta y que son densos en ella, esta condición se traduce en que hay números racionales "tan cerca como uno quiera" de cualquier punto sobre la recta. Sin embargo, hemos visto también que hay puntos sobre la recta, por ejemplo, el correspondiente a $\sqrt{2}$, que podemos construir usando el Teorema de Pitágoras, que no corresponde a ningún número racional. La intuición es que los racionales son como un harnero muy fino, pero que deja vacíos. Los números irracionales serán aquellos que llenan estos vacíos.

La presentación que haremos de los números reales fue propuesta por primera vez por Dedekind en [**2**], publicado en 1888. Una traducción de esta obra se puede estudiar en [**1**]. Esta no es la única manera de construir los números reales, sin embargo, es la que requiere de menos conocimientos de análisis y es netamente conjuntista, por lo que es muy adecuada para este libro.

Una *cortadura de Dedekind* o simplemente una *cortadura* [2] en los números racionales es un subconjunto A de $\mathbb{Q}$ que tiene las siguientes características.

1. $A \neq \emptyset$.
2. $A \neq \mathbb{Q}$.
3. Si $x <_{\mathbb{Q}} y$ e $y \in A$, entonces $x \in A$.
4. A no tiene un elemento máximo.

El ítem 3 dice que si un racional r está en la cortadura A, entonces todos los racionales más pequeños también lo están, por esto suele decirse que A es "cerrado hacia abajo".

Por ejemplo, si $r \in \mathbb{Q}$, entonces $C_r = \{x \in \mathbb{Q} : x <_{\mathbb{Q}} r\}$ es obviamente una cortadura.

También

$$C = \{r \in \mathbb{Q} : 0 \leq_{\mathbb{Q}} r \text{ y } r^2 <_{\mathbb{Q}} 2\} \cup C_0$$

es una cortadura. Vemos que $0 \in C$, luego $C \neq \emptyset$. Además $3 \notin C$, luego $C \neq \mathbb{Q}$.

Es fácil ver que C es cerrado hacia abajo. Supongamos que $y <_{\mathbb{Q}} x \in C$. Si $y <_{\mathbb{Q}} 0$, entonces $y \in C$ por definición. Si $0 \leq_{\mathbb{Q}} y \leq_{\mathbb{Q}} x$, entonces sabemos que $0 \leq_{\mathbb{Q}} y^2 \leq_{\mathbb{Q}} x^2 <_{\mathbb{Q}} 2$, la última desigualdad se cumple porque $x \in C$. Por lo tanto, $y \in C$, o sea, en cualquiera de los dos casos $y \in C$ y, por lo tanto, C es cerrado hacia abajo.

Demostraremos por reducción al absurdo que C no tiene máximo. Supongamos que sí lo tiene y llamémoslo m.

Es claro que $0 <_{\mathbb{Q}} m$, o si no, m no sería el máximo de C. Entonces $m^2 <_{\mathbb{Q}} 2$, y, por lo tanto, $0 <_{\mathbb{Q}} 2 - m^2$.

Para llegar a una contradicción podemos buscar un elemento de C que es más grande que m. ¿Existe un racional $h > 0$ tal que $(m+h)^2 < 2$? Para que esto suceda, debe verificarse que $m^2 + 2mh + h^2 < 2$, de hecho, basta que $h \leq_{\mathbb{Q}} 1$ de modo que $h^2 \leq_{\mathbb{Q}} h$. Así, si pedimos que $m^2 + 2mh + h < 2$, se cumplirá lo que necesitamos. Consideremos entonces el racional $h = \frac{2-m^2}{2m+1}$, entonces $0 <_{\mathbb{Q}} h \leq_{\mathbb{Q}} 1$. La última

[2] El lector encontrará frecuentemente en la literatura otras definiciones levemente distintas de cortadura. La más habitual es definir cortadura como un par (A, B) de subconjuntos de $\mathbb{Q}$ que tiene las siguientes características.

1. $A \neq \emptyset$ y $B \neq \emptyset$.
2. $A \cup B = \mathbb{Q}$.
3. Para todo $x \in A$ y todo $y \in B$, $x < y$.
4. A no tiene un elemento máximo.

Es fácil ver que esta definición no difiere mucho de la que hemos dado. En efecto, A es una cortadura en nuestro sentido, entonces el par $(A, \mathbb{Q} - A)$ es una cortadura de acuerdo con la nueva definición.

desigualdad se cumple pues, si no, $(m+1)^2 <_{\mathbb{Q}} 2$, o sea $m+1 \in C$ lo que contradice la maximalidad de m. Tenemos

$$(m+h)^2 = m^2 + 2mh + h^2 \leq_{\mathbb{Q}} m^2 + 2mh + h$$
$$= m^2 + (2m+1)h <_{\mathbb{Q}} m^2 + (2m+1)\frac{2-m^2}{2m+1} = 2\,,$$

es decir, $m+h \in C$. Pero $m <_{\mathbb{Q}} m+h$, lo que nuevamente contradice la maximalidad de m. Esta contradicción implica que el máximo no puede existir, lo que completa la demostración de que C es una cortadura.

Más adelante podremos demostrar que ésta no es igual a ninguna cortadura del tipo C_r para $r \in \mathbb{Q}$.

Definimos el conjunto de los *números reales* $\mathbb{R}$ como sigue:

$$\mathbb{R} = \{A \subseteq \mathbb{Q} \,:\, A \text{ es una cortadura}\}\,.$$

Hay una obvia inyección de $\mathbb{Q}$ en $\mathbb{R}$, a saber

$$\begin{array}{rcl} F \,:\, \mathbb{Q} & \longrightarrow & \mathbb{R} \\ r & \longmapsto & C_r = \{x \in \mathbb{Q} \,:\, x <_{\mathbb{Q}} r\}\,, \end{array}$$

de esta manera, al igual que los naturales pueden considerarse contenidos dentro de los enteros quienes están dentro de los racionales, estos últimos están contenidos dentro de los reales.

Cuando dotemos a los reales de una estructura algebraica y de orden, veremos que esta copia de $\mathbb{Q}$ en $\mathbb{R}$ respeta todas las propiedades esenciales de $\mathbb{Q}$.

Las cortaduras del tipo C_r para $r \in \mathbb{Q}$ se llaman cortaduras racionales. Las cortaduras que no son de ese tipo se llaman *cortaduras irracionales o números irracionales.*

2.4.1 Orden

Teorema 2.47. *La relación*

$$A \leq_{\mathbb{R}} B \quad \textit{si y solo si} \quad A \subseteq B\,,$$

es una relación de orden total, denso y sin primer ni último elemento en $\mathbb{R}$.

Demostración. Sabemos que la relación de ser subconjunto es un orden, luego si la restringimos sólo a conjuntos que son cortaduras, sigue siendo reflexiva, antisimétrica y transitiva. Más aún, se trata de un orden total porque si A y B, son dos cortaduras y $A \neq B$, entonces o bien existe $c \in A - B$ o bien existe $c \in B - A$. En el primer caso, c es cota superior de B o sea, para todo $x \in B$, $x \leq c$ y por 3 de la definición de cortadura, $x \in A$, es decir, $B <_{\mathbb{R}} A$. En el segundo caso obtenemos por el mismo argumento que $A <_{\mathbb{R}} B$.

Para verificar que es un orden denso, sean A y B dos reales tales que $A <_{\mathbb{R}} B$. Como esto significa que $A \subsetneq B$, debe entonces haber al menos un racional $b \in B - A$. Este no puede ser único por que si lo fuera, o sea, si $B = A \cup \{b\}$, entonces b sería

el máximo elemento de B, el que por definición no existe. Por lo tanto, hay al menos dos racionales b y $b' \in B - A$, podemos suponer que $b <_{\mathbb{Q}} b'$. Pero como los racionales son densos, existe algún c tal que $b <_{\mathbb{Q}} c <_{\mathbb{Q}} b'$ y entonces $A <_{\mathbb{R}} C_c <_{\mathbb{R}} B$.

Por último, es inmediato que $\mathbb{R}$ no tiene primer ni último elemento porque los racionales no lo tienen. Por ejemplo, si existiera un primer real P, o sea una cortadura que está contenida en todas las otras, como toda cortadura es no–vacía, existe un racional $p \in P$. Pero, entonces $C_p <_{\mathbb{R}} P$, contradiciendo la minimalidad de P. Para ver que no existe el último elemento U se usa la condición de que $U \neq \mathbb{Q}$. □

El siguiente teorema nos dice que la inmersión de $\mathbb{Q}$ en $\mathbb{R}$ respeta el orden de los racionales. Su demostración es inmediata de la definición

Teorema 2.48. *Dados dos racionales r y s,*

$$C_r \leq_{\mathbb{R}} C_s \quad \textit{si y solo si} \quad r \leq_{\mathbb{Q}} s\,.$$

2.4.2 Los reales y la recta

Como vimos en la sección anterior, hay una forma natural de poner los números racionales en correspondencia con puntos de una recta. Vimos también que los racionales no cubren la recta sino que dejan muchos vacíos, por ejemplo, $\sqrt{2}$, entre muchos otros. La idea intuitiva de la cortadura es tomar todos los racionales que son menores que un "vacío" y considerar ese conjunto como el "número" real que lo cubre.

2.4.3 La suma de números reales

Dados dos reales A y B definimos su *suma* como sigue.

$$A \oplus B = \{a + b \,:\, a \in A \ \text{ y } \ b \in B\}\,.$$

Debemos, antes que nada, verificar que la suma esté bien definida, en este caso, esto significa que el conjunto propuesto como la suma de las cortaduras A y B es, efectivamente una cortadura.

Lema 2.49. *El conjunto $A \oplus B$ definido más arriba es una cortadura.*

Demostración. Es claro que $A \oplus B \neq \emptyset$.

Por otra parte como $A \neq \mathbb{Q}$ existe $r \in \mathbb{Q}$ tal que para todo $a \in A$, $a <_{\mathbb{Q}} r$ y similarmente, existe $s \in \mathbb{Q}$ tal que para todo $b \in B$, $b <_{\mathbb{Q}} s$. Por lo tanto, $a + b <_{\mathbb{Q}} r + s$, luego $r + s \notin A \oplus B$. Se tiene entonces que $A \oplus B \neq \mathbb{Q}$.

Si $y \leq_{\mathbb{Q}} x = a + b \in A \oplus B$, entonces $y - a \leq_{\mathbb{Q}} x - a = b \in B$ y como B es una cortadura, $y - a \in B$, luego $y = a + (y - a) \in A \oplus B$.

Por último, debemos ver que $A \oplus B$ no tiene un elemento máximo. Supongamos, por el contrario, que sí lo tiene, llamémoslo m. Entonces, por definición, existen elementos $a_0 \in A$ y $b_0 \in B$ tales que $m = a_0 + b_0$. Ahora bien, como ni A ni B tienen elemento máximo, existen $a_1 \in A$ y $b_1 \in B$ tales que $a_0 <_{\mathbb{Q}} a_1$ y $b_0 <_{\mathbb{Q}} b_1$ luego $m = a_0 + b_0 <_{\mathbb{Q}} a_1 + b_1 \in A \oplus B$, lo que contradice la maximalidad de m. Esta

contradicción nos dice que nuestra suposición es falsa y, por lo tanto, $A \oplus B$ no tiene elemento máximo.

Esto completa la demostración de que $A \oplus B$ es una cortadura y, por lo tanto, la suma de números reales está bien definida. □

Probaremos ahora las principales propiedades de la suma de números reales y de su relación con el orden. Las demostraciones se siguen de hechos elementales de teoría de conjuntos y de las propiedades ya demostradas para las operaciones con números racionales. Como en el caso de los números enteros y de los números racionales, esto demuestra que los numeros reales constituyen un grupo bajo la suma.

Teorema 2.50. *La suma de números reales verifica las siguientes propiedades.*

1. *Es asociativa.*
2. *Es conmutativa.*
3. *El número real C_0 es neutro con respecto de la suma, es decir, para todo real A, $A \oplus C_0 = A$.*
4. *Todo número real A tiene un inverso aditivo, es decir, un número real y tal que $A \oplus y = C_0$. Este inverso es único y lo denotaremos $\ominus A$.*

Demostración.

1. Observar que

$$A \oplus (B \oplus C) = \{a + (b + c) : a \in A,\ b \in B,\ c \in C\}$$
$$= \{(a + b) + c : a \in A,\ b \in B,\ c \in C\} = (A \oplus B) \oplus C.$$

2. Observar que $A \oplus B = \{a + b : a \in A,\ b \in B\} = \{b + a : a \in A,\ b \in B\} = B \oplus A$.

3. Es inmediato que $A \oplus C_0 = \{a + b : a \in A,\ b \leq_{\mathbb{Q}} 0\} \subseteq A$, porque $a + b <_{\mathbb{Q}} a$ cuando $b <_{\mathbb{Q}} 0$.

Para probar la inclusión en el otro sentido, vemos que si $a \in A$, como A no tiene un elemento máximo, debe existir un número racional b tal que $a <_{\mathbb{Q}} b$ y $b \in A$. Pero, entonces, $a = b + (a - b)$, es decir, a es la suma de un elemento de A y un elemento de C_0, o sea $a \in A \oplus C_0$.

4. Definimos $\ominus A = \{x \in \mathbb{Q} :$ existe algún $b \notin A$ tal que $x <_{\mathbb{Q}} -b\}$.

Primero debemos ver que esta es una cortadura. Es claro que $\ominus A \neq \emptyset$.

Para ver que $\ominus A \neq \mathbb{Q}$, supongamos que no es así. Entonces $\ominus A = \mathbb{Q}$, es decir, dado $n \in \mathbb{N} \subseteq \mathbb{Q}$ existe $b \notin A$ tal que $n <_{\mathbb{Q}} -b$. Esto implica que $b <_{\mathbb{Q}} -n$ y dada la inmersión de $\mathbb{Q}$ en $\mathbb{R}$, tenemos $C_b <_{\mathbb{R}} C_{-n}$. Pero, además, $b \notin A$ implica que b es cota superior de A, luego $A <_{\mathbb{R}} C_b <_{\mathbb{R}} C_{-n}$ para todo n número natural. Es claro que esto implica que $A = \emptyset$.

Es inmediato de la definición que $\ominus A$ es cerrado hacia abajo.

Por último, $\ominus A$ no tiene máximo elemento, porque si $m \in \ominus A$ lo fuera, existiría $b \notin A$ tal que $m <_{\mathbb{Q}} -b$. Esto implica que $b <_{\mathbb{Q}} -m$ y como los racionales son densos,

existe r tal que $b <_{\mathbb{Q}} r <_{\mathbb{Q}} -m$, por lo tanto, $-r \in \ominus A$, porque $-r <_{\mathbb{Q}} -b$, pero también $m <_{\mathbb{Q}} -r$, lo que contradice la maximalidad de m.

Veamos ahora que, efectivamente, $\ominus A$ así definido actúa como inverso aditivo. Por las definiciones, si $x \in A \oplus (\ominus A)$, entonces $x = a + r$ con $a \in A$ y $r <_{\mathbb{Q}} -b$ para algún $b \notin A$.

Como $b \notin A$, para todo $z \in A$, $z <_{\mathbb{Q}} b$, en particular $a <_{\mathbb{Q}} b$ y tenemos $r <_{\mathbb{Q}} -b <_{\mathbb{Q}} -a$. Pero entonces $x = a + r <_{\mathbb{Q}} a + (-b) <_{\mathbb{Q}} a + (-a) = 0$, luego $x \in C_0$, o sea, $A \oplus (\ominus A) \leq_{\mathbb{R}} C_0$.

Por otra parte, si $x \in C_0$, $x <_{\mathbb{Q}} 0$ y como C_0 no tiene mayor elemento, consideramos un $y \in \mathbb{Q}$ tal que $x <_{\mathbb{Q}} y <_{\mathbb{Q}} 0$.

Como $0 <_{\mathbb{Q}} -y$, es inmediato que debe existir $a \in A$ tal que $a - y \notin A$, pues si no, A no sería acotado superiormente. Entonces $x - a <_{\mathbb{Q}} y - a = -(a - y) \notin A$, es decir, $x - a \in \ominus A$ y, por lo tanto, $x = a + (x - a) \in A \oplus (\ominus A)$. □

Las siguientes propiedades algebraicas de los números reales son consecuencia de las cuatro condiciones anteriores. El lector, que haya estudiado álgebra abstracta, verá inmediatamente que se trata de consecuencias de que los números reales son un grupo abeliano y podrá dar demostraciones algebraicas. Como dijimos en el prefacio, no hemos supuesto que el lector conoce esos temas. Por otra parte, la demostración que haremos de la primera propiedad, si bien es mucho más compleja que la algebraica, es más instructiva desde el punto de vista que hemos adoptado en este capítulo ya que es de carácter conjuntista.

Teorema 2.51. *Los números reales verifican las siguientes propiedades.*

1. $\ominus(\ominus A) = A$.
2. $\ominus(A \oplus B) = (\ominus A) \oplus (\ominus B)$.
3. *Vale la ley de cancelación para la suma, es decir, si* $x, y, z \in \mathbb{R}$ *son tales que* $x \oplus z = y \oplus z$, *entonces* $x = y$.
4. *Para todo* x *y todo* y *números reales,* $x \leq_{\mathbb{R}} y$ *si y solo si* $x \oplus z \leq_{\mathbb{R}} y \oplus z$. *La relación* $\leq_{\mathbb{R}}$ *puede reemplazarse por* $<_{\mathbb{R}}$.

Demostración.

1. Observemos primero que $y \in \ominus A$ si y solo si $y <_{\mathbb{Q}} -b$ para algún $b \notin A$ y que, por lo tanto, $y \notin \ominus A$ si y solo si para todo b tal que $y <_{\mathbb{Q}} -b$, debe ocurrir que $b \in A$.

Sea $x \in \ominus(\ominus A)$, entonces existe $y \in \mathbb{Q}$ tal que $y \notin (\ominus A)$ y $x <_{\mathbb{Q}} -y$, o lo que es lo mismo, $y <_{\mathbb{Q}} -x$. Pero ya vimos que $y \notin (\ominus A)$ significa que para todo z tal que $y <_{\mathbb{Q}} -z$, se tiene que $z \in A$, lo que unido a la otra condición, $y <_{\mathbb{Q}} -x$, implica que $x \in A$. Esto demuestra que $\ominus(\ominus A) \subseteq A$.

Recíprocamente, supongamos que $x \in A$. Entonces, como A no tiene máximo elemento, existe $u \in \mathbb{Q}$ tal que $x <_{\mathbb{Q}} u \in A$. Sea $y = -u$, es decir, $x <_{\mathbb{Q}} -y$. Para ver que $x \in \ominus(\ominus A)$ basta demostrar que $y \notin \ominus A$, o sea, queremos ver que si $y <_{\mathbb{Q}} -z$, entonces $z \in A$.

Ahora bien, consideremos un $z \in \mathbb{Q}$ tal que $y <_{\mathbb{Q}} -z$. Entonces, $z <_{\mathbb{Q}} -y = u \in A$ y como A es cerrado hacia abajo, esto implica que $z \in A$, o sea, hemos probado que si $y <_{\mathbb{Q}} -z$, entonces $z \in A$, que es lo que queríamos.

En resumen, $A \subseteq \ominus(\ominus A)$ y, por lo tanto, $A = \ominus(\ominus A)$.

Los otros ítemes se prueban en forma similar. □

2.4.4 El producto de números reales

La definición del producto de números reales es mucho menos natural que la de la suma o el orden. En realidad se trata de una definición ad–hoc, diseñada para que se cumplan las propiedades algebraicas conocidas de los reales.

Dados dos reales A y B definimos su *producto* como sigue.

$$A \odot B = \begin{cases} \{a\,b : a \in A, b \in B, 0 \leq_{\mathbb{Q}} a \text{ y } 0 \leq_{\mathbb{Q}} b\} \cup C_0, & \text{si } 0 \leq_{\mathbb{R}} A \text{ y } 0 \leq_{\mathbb{R}} B\,, \\ \ominus(A \odot (\ominus B))\,, & \text{si } 0 \leq_{\mathbb{R}} A \text{ y } B <_{\mathbb{R}} 0\,, \\ \ominus((\ominus A) \odot B)\,, & \text{si } A <_{\mathbb{R}} 0 \text{ y } 0 \leq_{\mathbb{R}} B\,, \\ \ominus((\ominus A) \odot (\ominus B))\,, & \text{si } A <_{\mathbb{R}} 0 \text{ y } B <_{\mathbb{R}} 0\,. \end{cases}$$

Lema 2.52. *El conjunto $A \odot B$ definido más arriba es una cortadura.*

Demostración. Supongamos que $0 \leq_{\mathbb{R}} A$ y $0 \leq_{\mathbb{R}} B$. Es claro que $A \odot B \neq \emptyset$ y que $A \odot B \neq \mathbb{Q}$. También es inmediato que $A \odot B$ es cerrado hacia abajo.

Supongamos ahora que $A \odot B$ tiene un máximo elemento m. Entonces, por definición, existen elementos $a_0 \in A$ y $b_0 \in B$, $0 <_{\mathbb{Q}} a_0$ y $0 <_{\mathbb{Q}} b_0$ tales que $m = a_0\,b_0$. Como ni A ni B tienen elemento máximo, existen $a_1 \in A$ y $b_1 \in B$ tales que $a_0 <_{\mathbb{Q}} a_1$ y $b_0 <_{\mathbb{Q}} b_1$ luego $m = a_0\,b_0 <_{\mathbb{Q}} a_1\,b_1 \in A \odot B$, lo que contradice la maximalidad de m.

Los otros tres casos se reducen al anterior. □

Ejemplo 2.53. El real $C = \{r \in \mathbb{Q} : 0 \leq_{\mathbb{Q}} r \text{ y } r^2 <_{\mathbb{Q}} 2\} \cup C_0$ definido anteriormente, verifica $C^2 = C \odot C = C_2$, o sea intuitivamente, C es un número real positivo que elevado al cuadrado da 2, es decir, C es la raíz cuadrada de 2.

Sea $z \in C^2$, sólo nos interesa $0 \leq_{\mathbb{Q}} z$. Entonces $z = xy$, con $0 \leq_{\mathbb{Q}} x \in C$ y $0 \leq_{\mathbb{Q}} y \in C$. Tenemos que

$$z = xy \leq_{\mathbb{Q}} (\max\{x, y\})^2 <_{\mathbb{Q}} 2\,,$$

por lo tanto, $z \in C_2$, es decir, $C^2 \leq_{\mathbb{R}} C_2$.

Por otra parte si $z \in C_2$, es decir, $z <_{\mathbb{Q}} 2$ existe $x \in C$ tal que $z <_{\mathbb{Q}} x^2 <_{\mathbb{Q}} 2$ porque C_2 no tiene máximo elemento. Por lo tanto, $z <_{\mathbb{Q}} x^2 \in C^2$ y como C^2 es una cortadura, $z \in C^2$. Esto completa la demostración y el número real C merece el nombre de raíz cuadrada de 2. Aunque no lo haremos aquí, podemos demostrar que este es el único real positivo cuyo cuadrado es 2.

Como bien vimos en la sección anterior, no existe un racional tal que su cuadrado es igual a 2, por lo tanto, $C \neq C_r$ para todo $r \in \mathbb{Q}$. Este proceso se puede repetir con otros números y otros exponentes obteniéndose así más y más números reales que no son racionales, o sea, números irracionales, estos son los que llenan los "vacíos" dejados por los racionales en la recta. En el próximo capítulo veremos que hay más irracionales que racionales. □

El siguiente teorema nos dice que el conjunto de los números reales distintos de cero, con la multiplicación, constituye un grupo abeliano y que el producto distribuye sobre la suma. Si unimos lo anterior con el Teorema 2.50 tenemos que los números reales constituyen un cuerpo.

Teorema 2.54. *El producto de números reales verifica las siguientes propiedades.*

1. *Es asociativo.*
2. *Es conmutativo.*
3. *El real C_1 es neutro con respecto a la multiplicación, es decir, para todo real x, $x \odot C_1 = x$.*
4. *Para todo real $x \neq C_0$, existe un único real y tal que $x \odot y = C_1$. Este número se llama* inverso multiplicativo *de x y habitualmente se le denota x^{-1}.*
5. *El producto de números reales es distributivo sobre la suma.*

Demostración. La mayoría de estas propiedades son heredadas de la correspondiente propiedad de los racionales.

3. Sea A un número real tal que $0 <_{\mathbb{R}} A$. Entonces

$$A \odot C_1 = \{a\, x : a \in A,\, 0 <_{\mathbb{Q}} a \ \text{ y } \ 0 \leq_{\mathbb{Q}} x <_{\mathbb{Q}} 1\} \cup C_0$$

y como $a\, x <_{\mathbb{Q}} a$ y $a \in A$, y también A es cerrado hacia abajo, $a\, x \in A$, o sea, $A \odot C_1 \subseteq A$.

Para demostrar la inclusión en el otro sentido, sea $a \in A$. Como es claro que $C_0 \subseteq A \odot C_1$, basta ver el otro caso. Si $a = 0$ también es obvio que $a \in A \odot C_1$. Nos queda sólo verificar el caso $0 <_{\mathbb{Q}} a$. Como A no tiene elemento máximo, existe un racional $b \in A$ tal que $a <_{\mathbb{Q}} b$. Por lo tanto, $0 \leq_{\mathbb{Q}} \frac{a}{b} <_{\mathbb{Q}} 1$ y, por consiguiente, $a = b\,\frac{a}{b} \in A \odot C_1$. Vemos que en cualquier caso $a \in A \odot C_1$, o sea, $A \subseteq A \odot C_1$ y ambos conjuntos son iguales.

El caso negativo se reduce al anterior, al tomar en cuenta los cambios de signo de la definición del producto.

4. Para $0 <_{\mathbb{R}} A$, definimos

$$A^{-1} = \{x \in \mathbb{Q} : x \leq_{\mathbb{Q}} 0\} \cup \left\{x \in \mathbb{Q} : x <_{\mathbb{Q}} \frac{1}{y} \ \text{ para algún } \ y \notin A\right\}.$$

Vemos que A^{-1} es una cortadura. Es claro que A^{-1} es no vacío y cerrado hacia abajo.

Para ver que A^{-1} es distinto de $\mathbb{Q}$, supongamos que no es así. Entonces, para cada $n \in \mathbb{N}$ existirá un $y \notin A$ tal que $n <_{\mathbb{Q}} \frac{1}{y}$ o, lo que es lo mismo, $y <_{\mathbb{Q}} \frac{1}{n}$. Pero esto implica que existen números racionales, tan pequeños como queramos, que no pertenecen a A. Por lo tanto, $A \leq_{\mathbb{R}} C_0$, lo que contradice nuestra elección de A.

Supongamos que A^{-1} tiene un máximo m. Entonces, dado que $m \in A^{-1}$, existe $y \notin A$ tal que $m <_{\mathbb{Q}} \frac{1}{y}$. Afirmamos que $\frac{1}{m}$ es el máximo elemento de A. En efecto, si $\frac{1}{m}$ no fuera el máximo de A, existiría un $x \in A$ tal que $m <_{\mathbb{Q}} x$, lo que nos lleva a que $y <_{\mathbb{Q}} \frac{1}{m} <_{\mathbb{Q}} x$, lo que es claramente imposible dado que y es una cota superior de A. Hemos probado que bajo la suposición de que A^{-1} tiene un máximo, A también tendría un máximo elemento lo que, como sabemos, no puede existir.

Es claro que el inverso así definido es único.

Para ver que $A \odot A^{-1} = C_1$, sean $a \in A$ y $b \in A^{-1}$, a y b positivos. Entonces debe existir $y \notin A$ tal que $b <_{\mathbb{Q}} \frac{1}{y}$. Pero, además, $a <_{\mathbb{Q}} y$ porque $y \notin A$. Multiplicando la primera inecuación por a y la segunda por $\frac{1}{y}$, tenemos

$$a\,b <_{\mathbb{Q}} a \cdot \frac{1}{y} <_{\mathbb{Q}} y \cdot \frac{1}{y} = 1\,,$$

por lo tanto, $a\,b <_{\mathbb{Q}} 1$, es decir, $A \odot A^{-1} \subseteq C_1$.

La demostración de la inclusión en el otro sentido es un problema mucho más difícil, cae en el terreno del análisis y escapa a los objetivos de este texto. La incluimos aquí porque es un resultado difícil de encontrar en los libros más habituales. Invitamos al lector a seguirla y a profundizar en estos temas.

Como A es una cortadura no tiene máximo elemento y el complemento de A no tiene mínimo elemento. Es así que tenemos elementos dentro de A y fuera de él, que están, entre sí, tan cerca como se quiera. Más precisamente, vemos que para cada número natural n podemos encontrar un $x \in A$ y un $y \notin A$ tales que $y - x <_{\mathbb{Q}} \frac{a}{n}$, donde a es un elemento fijo de A que podemos tomar muy pequeño. Obsérvese que si tomamos un $u \in A$ y un $v \notin A$, con $x <_{\mathbb{Q}} u <_{\mathbb{Q}} v <_{\mathbb{Q}} y$, entonces $v - u <_{\mathbb{Q}} y - x$, de tal manera que tomando x más y más grande e y más y más chico, la diferencia $y - x$ disminuye tanto como queramos. De esta manera, podemos encontrar tales x e y de modo que $a <_{\mathbb{Q}} x$. Si hacemos esto obtendremos

$$y - x <_{\mathbb{Q}} \frac{a}{n} <_{\mathbb{Q}} \frac{x}{n}\,.$$

Esto tiene consecuencias importantes ya que obtenemos $y <_{\mathbb{Q}} x + \frac{x}{n} = \frac{xn+x}{n}$, o, lo que es lo mismo,

$$\frac{n}{(n+1)\,x} <_{\mathbb{Q}} \frac{1}{y}\,,$$

es decir, $\frac{n}{(n+1)\,x} \in A^{-1}$. Pero entonces

$$\frac{n}{n+1} = x \cdot \frac{n}{(n+1)\,x} \in A \odot A^{-1}$$

además, esto es así para todo n.

Dado que para cualquier racional $r <_{\mathbb{Q}} 1$, existe un número natural tal que $r <_{\mathbb{Q}} \frac{n}{n+1}$ y que las cortaduras son cerradas hacia abajo, obtenemos que $C_1 \subseteq A \odot A^{-1}$.

Para el caso $A <_{\mathbb{R}} 0$, definimos $A^{-1} = \ominus(\ominus A)^{-1}$ y todo se reduce al caso anterior. □

Las siguientes propiedades valen en cualquier cuerpo. Conviene, sin embargo, para nuestro propósito hacer demostraciones dentro de la teoría de conjuntos.

Teorema 2.55. *El producto de números reales verifica las siguientes propiedades.*

1. *Si* $a \neq C_0$*, entonces la ecuación* $a \odot x = b$ *tiene solución única* $x = a^{-1}b$.
2. *Para todo real* x, $x \odot C_0 = C_0$.
3. *Vale la ley de cancelación para la multiplicación por un real distinto de cero, es decir, si* $x, y, z \in \mathbb{R}$, $z \neq 0$ *y* $x \odot z = y \odot z$, *entonces* $x = y$.
4. *En los números reales no hay divisores del cero, es decir, si* x, y *son dos reales tales que* $x \odot y = 0$, *entonces o bien* $x = 0$ *o bien* $y = 0$.
5. *Si* $x, y \in \mathbb{R}$, $(-x) \odot (-y) = x \odot y$.

Demostración.

1. La demostración es idéntica a la del caso racional.

5. La definición de producto fue hecha para que esto se cumpliera. □

2.4.5 El "axioma" del supremo

El siguiente teorema es el conocido Axioma del Supremo de la teoría clásica de los números reales y es uno de los rasgos que caracterizan a los reales. Su nombre puede mover a confusión porque no se trata de un axioma de la teoría de conjuntos, sino de un axioma de la teoría de cuerpos ordenados completos. Resulta que en el modelo de los números reales que hemos construido dentro de la teoría de conjuntos, este axioma es un teorema muy sencillo.

Teorema 2.56. *Todo conjunto de números reales no vacío y acotado superiormente tiene un supremo.*

Demostración. Sea A un conjunto no vacío y acotado de números reales. Entonces

$$c = \{x \in \mathbb{Q} : C_x <_{\mathbb{R}} a \text{ para algún } a \in A\}$$

es el supremo de A. En efecto, c es obviamente no vacío y $c \neq \mathbb{Q}$ porque A es acotado superiormente. También es inmediato de la definición que c es cerrado hacia abajo. Falta verificar que c no tiene elemento máximo. Si m fuera el máximo de c, entonces $C_m <_{\mathbb{R}} a$, para algún $a \in A$, es decir, $m \in a$, y m sería el máximo elemento de a pero ésta es una cortadura y, por lo tanto, no tiene máximo, o sea,

se produce una contradicción. Para ver que c es cota superior, consideremos $a \in A$, entonces por definición todo $x \in a$ pertenece a c, es decir, $a \subseteq c$, o sea $a \leq_{\mathbb{R}} c$. Para ver que c es la menor cota superior, sea d otra cota superior. Entonces todo $a \in A$ verifica $a \subseteq d$ luego si $x \in c$, entonces $x \in d$, es decir, $c \subseteq d$, o sea $c \leq_{\mathbb{R}} d$. □

2.4.6 Ejercicios

1. Demostrar que el orden definido por la relación de subconjunto restringido a las cortaduras es un orden total.
2. Demostrar la propiedad arquimediana de los números reales, a saber, si a, $b \in \mathbb{R}$, y $0 <_{\mathbb{R}} a$, entonces existe un número natural n tal que $b <_{\mathbb{R}} n \cdot a$.
3. Demostrar todas las afirmaciones que no se demostraron en el Teorema 2.50 y 2.51.
4. Demostrar todas las afirmaciones que no se demostraron en los Teoremas 2.54 y 2.55.
5. Demostrar que los siguientes conjuntos son cortaduras.
   a) $\{r \in \mathbb{Q} : 0 \leq_{\mathbb{Q}} r \text{ y } r^2 <_{\mathbb{Q}} 3\} \cup C_0$.
   b) $\{r \in \mathbb{Q} : 0 \leq_{\mathbb{Q}} r \text{ y } r^2 <_{\mathbb{Q}} n\} \cup C_0$.
   c) $\{r \in \mathbb{Q} : 0 \leq_{\mathbb{Q}} r \text{ y } r^3 <_{\mathbb{Q}} 2\} \cup C_0$.
   d) $\{r \in \mathbb{Q} : 0 \leq_{\mathbb{Q}} r \text{ y } r^p <_{\mathbb{Q}} 2\} \cup C_0$, para algún p.
6. Demostrar que las cortaduras del problema anterior verifican respectivamente:
   a) $r^2 = 3$.
   b) $r^2 = a$, para cualquier número real positivo a.
   c) $r^3 = 2$.
   d) $r^p = 2$, para cualquier número natural p.

Capítulo 3: Cardinalidad

¿Qué hacemos cuando contamos? ¿Cuál es la operación mental realizada al enumerar objetos? ¿Qué significa la frase: "En esta sala hay treinta personas"? ¿Qué significa el "número de elementos de un conjunto"? De alguna manera tenemos la sensación de andar en círculos: contar significa dar el número de elementos, pero el número de elementos se obtiene contando. Aparentemente para contar necesitamos haber desarrollado los números naturales, los que serían una especie de representante de todos los conjuntos que tienen un cierta cantidad de elementos. Por ejemplo, el número dos representa a todos los pares, el número tres a todos los tríos, etc. Detrás del contar hay una noción más básica, esta es la de *equinumerosidad*, intuitivamente, tener la misma cantidad de elementos. Veremos que, para saber si dos conjuntos tienen el mismo número de elementos, no se necesita siquiera conocer el concepto de número. La siguiente historia imaginaria es bien conocida.

Un pastor prehistórico tiene un rebaño de ovejas. Obviamente este individuo no sabe "contar" más allá de cuatro y no sabe nada de aritmética. Cada mañana cuando saca su rebaño a pastar pone en un canasto una piedra por cada oveja que sale. Al regresar en la noche, saca una piedra por cada oveja que entra al redil. Si sobran piedras habrá perdido al menos una oveja descarriada y deberá ir a buscarla, si faltan piedras, parió una oveja y habrá fiesta. Vemos que sin saber nada de matemática (¿realmente no sabe nada de matemática?) nuestro primitivo pastor puede manejar un problema de conteo no trivial. A veces es más importante saber si dos conjuntos son equinumerosos, que saber su número de elementos. Como veremos más adelante, esta idea es la que nos permite generalizar la noción de cantidad de elementos a los conjuntos infinitos.

Dos conjuntos A y B son *equinumerosos*[1] si existe una biyección entre ellos.

La biyección hace corresponder a cada elemento de cada conjunto un único elemento del otro, sin que sobren elementos en ninguno de ellos. Se captura así la noción intuitiva de tener la misma cantidad de elementos.

Decimos también que un conjunto A tiene *cardinalidad menor o igual* que la de un conjunto B si existe una función inyectiva entre ellos. Esto suele denotarse $A \preceq B$.

[1]Muchos autores prefieren la palabra *equipotente* en lugar de *equinumeroso*.

Un conjunto se dirá *finito* si es equinumeroso con algún número natural n, o sea, hay una biyección

$$f : A \longrightarrow \{0, 1, 2, 3, \ldots, n-1\} .$$

Dicho n se llama el *cardinal o la cardinalidad* del conjunto A. Usaremos el símbolo $\sharp A$ para denotar la cardinalidad del conjunto A. Por ejemplo, $\sharp\emptyset = 0$ y $\sharp\{1, 2, 4\} = 3$. En general debe resultar evidente que para cualquier número natural n, (recuerde que n es un conjunto), $\sharp n = n$. Esto es otra particularidad de la teoría, los cardinales de un conjunto finito son conjuntos.

Si no existe una biyección entre el conjunto y algún número natural, entonces el conjunto se dirá *infinito*. Por ejemplo, es fácil ver que no puede haber ninguna biyección entre el conjunto $\mathbb{N}$ de todos los números naturales y un número natural cualquiera. En efecto, si tal biyección existiera, digamos

$$f : \mathbb{N} \longrightarrow \{0, 1, 2, 3, \ldots, n-1\} ,$$

debe existir un número natural m más grande que todos los números

$$f^{-1}(0), f^{-1}(1), \ldots, f^{-1}(n-1) ,$$

pero como f es inyectiva, no podríamos asignar ningún valor a $f(m)$. Esto prueba que $\mathbb{N}$ es infinito.

En un plano más intuitivo, otros ejemplos de conjunto infinito son los números reales $\mathbb{R}$, los puntos sobre una recta, las rectas de un plano, etc.

Lema 3.1. *La relación de equinumerosidad entre los conjuntos de un conjunto dado es una relación de equivalencia.*

Demostración. Se deja al lector. □

Debemos observar que todo conjunto finito tiene un único cardinal. De no ser así, por la transitividad de la relación de equinumerosidad, habría dos números naturales n y m (digamos $n < m$) y una biyección

$$f : \{0, 1, 2, \ldots, n\} \longrightarrow \{0, 1, 2, \ldots, n, n+1, \ldots, m\} ,$$

lo cual es intuitivamente imposible, aunque sea algo engorroso de escribir formalmente.

Si un conjunto es finito, con tiempo y paciencia podemos "contarlo", es decir, encontrar su cardinalidad. Pero, ¿qué pasa con conjuntos no finitos? Esto lo estudiaremos en la próxima sección.

Un teorema interesante es el siguiente.

Teorema 3.2. *Si A y B son dos conjuntos finitos, entonces:*

1. *Si los conjuntos son disjuntos,*

$$\sharp(A \cup B) = \sharp A + \sharp B .$$

2. *En general*

$$\sharp(A \cup B) \ + \ \sharp(A \cap B) = \sharp A \ + \ \sharp B \ .$$

Demostración. Ejercicio. □

Ejemplo 3.3. Consideremos los conjuntos $A = \{n \in \mathbb{N} : 1 \leq n \leq 100$ y n es par$\}$ y $B = \{n \in \mathbb{N} : n$ es múltiplo de 5 y menor o igual que 100 $\}$. Entonces $\sharp A = 50$, $\sharp B = 20$, pero de estos últimos la mitad son pares, es decir, $\sharp(A \cap B) = 10$ y, por lo tanto, $\sharp(A \cup B) = 60$.

□

3.1 Conjuntos infinitos

Dijimos que un conjunto que no es finito se dirá infinito. ¿Cómo podemos asignar una cardinalidad a un conjunto infinito?, ¿tienen todos los conjuntos infinitos la misma cardinalidad?

Observemos que la noción de equinumerosidad introducida en la sección anterior no depende de que los conjuntos sean finitos o infinitos. Por ejemplo, consideremos el conjunto $P = \{0, 2, 4, \ldots\}$ de los números pares. $\mathbb{N}$ y P son equinumerosos como lo demuestra la siguiente biyección:

$$\begin{array}{ccccccccc} 0 & 1 & 2 & 3 & & & n & & \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & & \updownarrow & \cdots & \\ 0 & 2 & 4 & 6 & & & 2n & & \end{array}$$

Con este ejemplo surge la primera particularidad de los conjuntos infinitos: una parte puede tener la misma cantidad de elementos que el todo. Obviamente esto no es cierto para conjuntos finitos.

Teorema 3.4. *Si un conjunto es equinumeroso con un subconjunto propio, entonces es infinito.*

El teorema anterior es importante en la historia del infinito. R. Dedekind la propuso como definición de conjunto infinito. En cierto sentido es una definición muy buena, porque no apela a los números naturales sino que es intrínseca, es decir, depende sólo del conjunto en cuestión y no de otros conjuntos que hayamos construido. Sin embargo, para caracterizar plenamente a los conjuntos infinitos, el recíproco también debería ser cierto. El problema es que para demostrar este recíproco debemos apelar al axioma más delicado de la teoría de conjuntos, el Axioma de Elección. Esto lo veremos en el próximo capítulo.

Ejemplos 3.5.

Los siguientes conjuntos son equinumerosos con el conjunto de los números naturales.

1. $I = \{1, 3, 5, 7, \ldots\}$
2. $3\mathbb{N} = \{0, 3, 6, 9, \ldots\}$

3. $\mathbb{Z}$, como demuestra la siguiente biyección.

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & & \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & \\ 0 & 1 & -1 & 2 & -2 & & \end{array}$$

Como se ve, relacionamos los impares con los enteros positivos y los pares con los negativos. Luego $\mathbb{N}$ y $\mathbb{Z}$ son equinumerosos.

4. El producto cartesiano $\mathbb{N} \times \mathbb{N}$, de los pares ordenados de números naturales. En efecto,

$$\begin{array}{rccl} f & : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & & (n, m) & \longmapsto & 2^n(2m+1) - 1 \end{array}$$

es biyectiva.

Para verificar que f es inyectiva, supongamos que $f(n, m) = f(p, q)$. Entonces

$$\begin{array}{rcl} 2^n(2m+1) - 1 & = & 2^p(2q+1) - 1 \\ 2^n(2m+1) & = & 2^p(2q+1) \end{array}$$

suponiendo $n > p$

$$2^{n-p}(2m+1) = 2q+1$$

entonces, el término de la izquierda sería par y el derecha sería impar, lo que es imposible. Algo similar ocurre si $n < p$. Luego $n = p$ y podemos cancelar. Queda

$$\begin{array}{rcl} 2m+1 & = & 2q+1 \\ m & = & q \end{array}$$

es decir, f es inyectiva.

La comprobación de que f es sobreyectiva es mucho más compleja y apela al Teorema Fundamental de la Aritmética (ver [**7**]).

Observamos que $0 = f(0, 0)$ y $1 = f(1, 0)$. Para los números mayores que 1 recordamos que todo natural mayor que 1 se descompone de manera única como producto de números primos

$$2^n {p_1}^{m_1} {p_2}^{m_2} \cdots {p_k}^{m_k} ,$$

donde $n \geq 0$, los m_i son mayores que 0 y los p_i son ciertos primos impares. Entonces, dado $r \in \mathbb{N}$ consideramos la descomposición prima anterior del número $r+1$. Observamos que como los p_i son impares, su producto es impar y mayor que 1. Hacemos

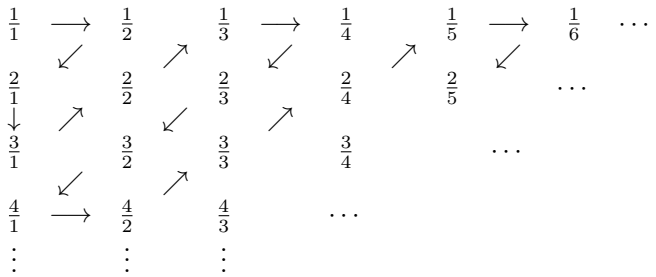
$$2m + 1 = {p_1}^{m_1} {p_2}^{m_2} \cdots {p_k}^{m_k} .$$

Vemos entonces que

$$r = 2^n {p_1}^{m_1} {p_2}^{m_2} \cdots {p_k}^{m_k} - 1 = 2^n(2m+1) - 1 = f(n, m) ,$$

y f es sobreyectiva.

5. Otro ejemplo de las curiosidades de los conjuntos infinitos es la siguiente. Consideremos el conjunto de los números racionales positivos y ordenémoslos según el cuadro siguiente.



Si asignamos a cada número natural un racional siguiendo la flecha (y omitiendo las repeticiones) obtendremos una biyección entre este conjunto y $\mathbb{N}$. Más aún, si hacemos lo mismo con los números negativos y las fracciones negativas, $\mathbb{Z}$ es equinumeroso con $\mathbb{Q}$ el conjunto de los números racionales. Esto es sumamente extraño a primera vista ya que entre dos números racionales, digamos 5 y 6, ¡hay infinitos racionales! □

Diremos que un conjunto es *numerable* si es equinumeroso con el conjunto de los números naturales.

Observemos que si A es un conjunto numerable, entonces existe una biyección $f : \mathbb{N} \longrightarrow A$, de modo que podemos hacer una "lista infinita"[2] de los elementos de A donde $a_0 = f(0),\ a_1 = f(1), \ldots, a_n = f(n), \ldots$. A menudo describimos los conjuntos numerables como

$$A = \{a_0, a_1, \ldots, a_n, \ldots\} .$$

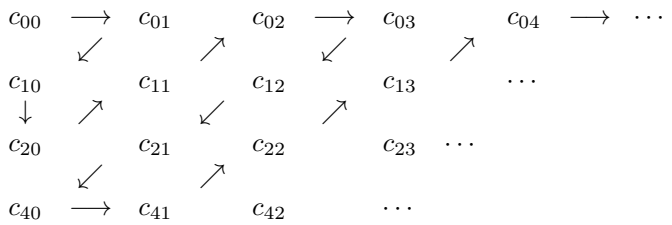
La construcción de la biyección entre los números naturales y los números racionales se puede usar para demostrar un teorema general.

Teorema 3.6. *La unión de un conjunto numerable de conjuntos numerables es un conjunto numerable.*

Demostración. Para cada $n \in \mathbb{N}$ vamos a considerar un conjunto C_n que a su vez es numerable. Podemos escribirlo entonces como $C_n = \{c_{n0}, c_{n1}, \ldots, c_{nk}, \ldots\}$. Vamos a suponer que todos ellos son disjuntos de a pares, es decir, si $n \neq m$, entonces $C_n \cap C_m = \emptyset$. Ordenemos ahora los conjuntos como anteriormente hicimos con los racionales. Los elementos de C_0 en la primera fila, los de C_1 en la segunda, etc. Entonces todos los elementos de la unión de los conjuntos estará en alguna fila y

[2]Advertimos a aquellos lectores que tienen conocimientos de Teoría de Computabilidad que usamos la palabra "lista" en un sentido no técnico. Nada nos importa si la función f es efectivamente calculable.

alguna columna de este cuadrado infinito. La biyección está dada por la flecha que pasa por todos ellos en un recorrido siguiendo las diagonales.



Observemos que ésta es esencialmente la misma idea que usamos para demostrar la numerabilidad del conjunto de los números racionales.

Si los conjuntos C_n no fuesen disjuntos a pares, consideramos en su lugar los conjuntos $C_n \times \{n\}$. Estos sí son disjuntos a pares y para cada n, C_n y $C_n \times \{n\}$ son obviamente equinumerosos. Es claro que el resultado no se ve afectado si usamos los segundos en lugar de los primeros. □

El lector podrá también comprobar que la función que al k–ésimo elemento del n–ésimo conjunto, es decir, a c_{nk}, asigna el número $2^n(2k+1)-1$ es una biyección entre la unión de los C_n y $\mathbb{N}$. Esta biyección no corresponde a la construida en el diagrama, ¿cómo se relaciona este problema con el anterior en donde apareció una función similar?

Debemos hacer notar que en esta demostración hemos usado subrepticiamente el ya mencionado Axioma de Elección que estudiaremos en el Capítulo 4. Allí discutiremos este ejemplo nuevamente. Adelantamos aquí que hemos usado el hecho de que para cada conjunto numerable hay una biyección con $\mathbb{N}$ y hemos escogido una particular, para cada uno de los infinitos conjuntos al mismo tiempo.

Es interesante destacar que los fundadores de la Teoría de Conjuntos tardaron muchos años en notar que este tipo de prácticas involucra un axioma especial.

Ejemplos 3.7.

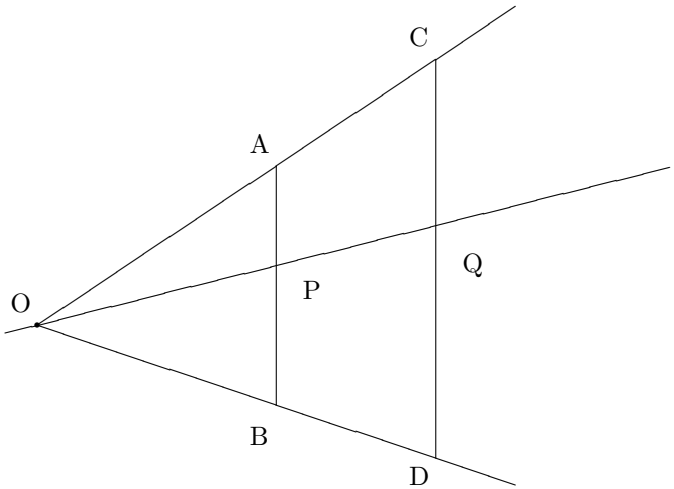
Hacemos una pausa en nuestra teoría, para ilustrar el concepto de equinumerosidad con ejemplos que no involucran conjuntos en el sentido técnico que estamos desarrollando, sino de conjuntos del ámbito de la matemática intuitiva que el lector ha estudiado.

1. Dos segmentos $\overline{AB}$ y $\overline{CD}$, sin importar su largo, tienen el mismo número de puntos, como lo demuestra la figura siguiente. Las rectas $\overleftrightarrow{AC}$ y $\overleftrightarrow{BD}$ se cortan en O. Definimos la siguiente biyección entre $\overline{AB}$ y $\overline{CD}$. Para cada punto P sobre $\overline{AB}$ trazamos la recta $\overleftrightarrow{OP}$. Esta cortará al segmento $\overline{CD}$ en Q, esta es la imagen del punto P.

   Es claro que la función está bien definida porque por O y P pasa una única recta y ésta corta a $\overline{CD}$ en un único punto.

La función es inyectiva ya que a puntos distintos P y P' le corresponden rectas distintas $\overleftrightarrow{OP}$ y $\overleftrightarrow{OP'}$ que cortaran a CD en puntos distintos Q y Q'.

También vemos que es sobreyectiva porque para cualquier punto Q del segmento $\overline{CD}$ podemos encontrar su preimagen como la intersección de la recta $\overleftrightarrow{OQ}$ con el segmento $\overline{AB}$.



2. El ejemplo anterior demuestra que todos los intervalos cerrados de números reales son equinumerosos. Hacemos notar que una demostración geométrica similar demuestra que todo intervalo abierto tiene la misma cardinalidad. Veamos ahora que el intervalo cerrado $[0,1]$ también es equinumeroso con el intervalo abierto $(0,1)$.

   Observemos que $\{\frac{1}{n} : n > 0\} \subseteq (0,1)$.

   Definimos la función

$$f : [0,1] \longrightarrow (0,1)$$

$$f(x) = \begin{cases} \frac{1}{2} & \text{si } x = 0, \\ \frac{1}{3} & \text{si } x = 1, \\ \frac{1}{n+2} & \text{si } x = \frac{1}{n},\ n > 1\,, \\ x & \text{en otro caso.} \end{cases}$$

   Dejamos al lector la comprobación de que ésta es una biyección.

3. Todo intervalo, abierto o cerrado es equinumeroso con el conjunto de los números reales. Esto es lo mismo que decir que la recta ilimitada es equinumerosa con cualquier intervalo, por pequeño que sea. Para demostrar esto basta recordar que la función trigonométrica $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \longrightarrow \mathbb{R}$ es una biyección. Esto, unido a los dos resultados anteriores, prueba la afirmación.

Hemos encontrado algunos conjuntos infinitos. También hemos demostrado que algunos de ellos son equinumerosos entre sí, pero ¿existen distintas cardinalidades infinitas? Por ejemplo, ¿es el conjunto de los números reales $\mathbb{R}$ equinumeroso con $\mathbb{N}$?

Responderemos esta última pregunta: hay más números reales que naturales. El argumento empleado aquí es conocido como el *método diagonal de Cantor*. Cantor lo propuso para demostrar el próximo teorema, aunque no fue ésta su primera demostración. El método ha sido aplicado a numerosos problemas y merece un estudio más detallado, pero que escapa a las posibilidades de este libro.

Teorema 3.8. *El conjunto de los números reales no es numerable.*

Demostración. Para ello, por un ejemplo de la lista anterior, basta que consideremos sólo los números reales en el intervalo abierto $(0, 1)$. Supongamos que éste es numerable. Entonces los puedo ordenar en una lista escribiéndolos en su representación decimal[3] .

$$\begin{array}{rcl} r_1 & = & 0, \mathbf{r_{11}}\ r_{12}\ r_{13}\ r_{14}\ \cdots \\ r_2 & = & 0, r_{21}\ \mathbf{r_{22}}\ r_{23}\ r_{24}\ \cdots \\ r_3 & = & 0, r_{31}\ r_{32}\ \mathbf{r_{33}}\ r_{34}\ \cdots \\ r_4 & = & 0, r_{41}\ r_{42}\ r_{43}\ \mathbf{r_{44}}\ \cdots \\ \vdots & & \vdots \qquad\qquad \ddots \end{array}$$

(Hemos empezado la lista con el subíndice 1 en lugar del 0 por pura comodidad notacional).

O sea, r_{nk} es la k–ésima cifra decimal del n–ésimo real de $(0, 1)$. En esta lista estarían *todos* los números reales entre 0 y 1. Sin embargo, si tomamos el número construido como sigue

$$r = 0, a_1\ a_2\ a_3\ \cdots$$

donde

$$a_i = \begin{cases} 2 & \text{si } r_{ii} = 5, \\ 5 & \text{si } r_{ii} \neq 5\,, \end{cases}$$

[3]No hemos desarrollado dentro de nuestra teoría axiomática la noción de representación decimal, tampoco es nuestra intensión hacerlo. Apelamos aquí a los conocimientos intuitivos del lector. En rigor hay que cuidarse de no duplicar ciertos números. Por ejemplo $0,1 = 0,09999\cdots$. Esto no es problema, en estos casos podemos adoptar la convención de usar la representación con el 9 periódico.

entonces es inmediato que r es distinto de todos los números que aparecen en la lista ya que a_1 es distinto de la primera cifra decimal de r_1, a_2 es distinto de la segunda cifra decimal de r_2, a_3 es distinto de la tercera cifra decimal de r_3, etc.

Sin embargo, obviamente r es un número real entre 0 y 1, es decir, la lista no estaba completa, o sea, $\mathbb{R}$ tiene más elementos que $\mathbb{N}$. □

Vemos que hay por lo menos dos cardinalidades infinitas distintas. La verdad es que existen muchas cardinalidades infinitas. De hecho, ¡existen infinitas cardinalidades infinitas! Para demostrar este hecho veamos el siguiente teorema.

Teorema 3.9. Teorema de Cantor.
El conjunto $\mathcal{P}(A)$ de todos los subconjuntos de A, no es equinumeroso con A.

Demostración. Supongamos por el contrario que A y $\mathcal{P}(A)$ son equinumerosos. Entonces existe una biyección $f : A \longrightarrow \mathcal{P}(A)$.

Consideremos ahora el siguiente subconjunto de A:

$$C = \{x \in A : x \notin f(x)\}.$$

Como $C \subseteq A$ y f es sobreyectiva, existe un $c \in A$ tal que, $f(c) = C$. La pregunta es ¿pertenece c a C? Veamos, si $c \in C$ por definición de C, $c \notin f(c) = C$, lo que es una contradicción. Luego $c \notin C$. Pero en tal caso $c \notin f(c)$ y, por definición, $c \in C$, nuevamente se obtiene una contradicción. Es decir, tanto $c \in C$ como $c \notin C$ son contradictorios. ¿De dónde viene el problema? Sólo de suponer que A y $\mathcal{P}(A)$ son equinumerosos, luego debemos rechazar esta suposición. □

Vemos entonces que hay conjuntos infinitos, por ejemplo, $\mathbb{N}$ y $P(\mathbb{N})$, que no son equinumerosos, es decir, hay distintos tipos de cardinalidad infinita. La pregunta obvia es, ¿pueden compararse estos infinitos?

Intuitivamente, si apareamos los elementos de un conjunto como hacía nuestro pastor primitivo, y uno de los conjuntos se acaba mientras en el otro sobran, podemos decir que el primero tiene menos o a lo sumo, la misma cantidad de elementos que el segundo. Esta idea, que puede aplicarse tanto a conjuntos finitos como infinitos, se reduce a la existencia de una función inyectiva del primer conjunto en el segundo.

Ejemplos 3.10.

1. Es claro que la función
$$\begin{array}{rccc} f & : & A & \longrightarrow & \mathcal{P}(A) \\ & & a & \longmapsto & \{a\} \end{array}$$
es una función inyectiva, luego A tiene cardinalidad menor o igual que $\mathcal{P}(A)$, pero como por el Teorema anterior no puede ser igual, debe ser estrictamente menor.
2. De la misma manera, si $A \subseteq B$, entonces A tiene a lo sumo la misma cardinalidad que B ya que la identidad es una función inyectiva de A en B.

3. Sin embargo, hay conjuntos, por ejemplo, $\mathbb{N}$ y $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$, para los que hay funciones inyectivas

$$\begin{aligned} f\ :\ \mathbb{N} &\longrightarrow \mathbb{N}\times\mathbb{N}\times\mathbb{N} \\ n &\longmapsto (n,0,0) \end{aligned}$$

$$\begin{aligned} g\ :\ \mathbb{N}\times\mathbb{N}\times\mathbb{N} &\longrightarrow \mathbb{N} \\ (n,m,q) &\longmapsto 2^n\,3^m\,5^q\,, \end{aligned}$$

es decir, $\mathbb{N}$ tiene a lo sumo la misma cantidad de elementos que $\mathbb{N}\times\mathbb{N}\times\mathbb{N}$ y viceversa. Obsérvese que ninguna de las funciones es sobreyectiva.

El último ejemplo nos indica que hay conjuntos tales que ambos tienen a lo sumo la cardinalidad del otro. Vamos a precisar qué relación hay entre esto y la de equinumerosidad. El próximo teorema es quizás el más importante sobre comparación de cardinalidades entre conjuntos infinitos (aunque también vale para conjuntos finitos).

Teorema 3.11. Teorema de Cantor–Schroeder–Bernstein.[4]
Supongamos que existen funciones inyectivas $f\ A :\longrightarrow B$ *y* $g\ B :\longrightarrow A$. *Entonces* A *y* B *son equinumerosos.*

Demostración. Sean $f\ :\ A\longrightarrow B$ y $g\ :\ B\longrightarrow A$ funciones inyectivas y para cada $n\in\mathbb{N}$ definamos

$$A_0 = A - g[B] \qquad \text{y} \qquad A_{n+1} = g[f[A_n]\,]\,.$$

Si A_0 fuese vacío, entonces g sería una biyección y no habría nada que demostrar. Luego supongamos que A_0 es no vacío. Debe observarse que los A_i son todos disjuntos a pares, es decir, para $i\neq j$, $A_i\cap A_j=\emptyset$, debido a que tanto f como g son inyectivas. Definimos

$$h(x) = \begin{cases} f(x) & \text{si } x\in A_n, \text{ para algún } n\,, \\ g^{-1}(x) & \text{si no.} \end{cases}$$

Observamos que h está definida para todo $a\in A$. Si $a\notin A_n$ para ningún n, en particular, $a\notin A_0$, o sea $a\in g[B]$, es decir, $a=g(b)$ para algún $b\in B$, luego $h(a)=g^{-1}(g(b))=b$.

Veamos ahora que h es inyectiva. Consideremos dos elementos distintos a, $a'\in A$. Hay varios casos. Si ambos pertenecen a $\bigcup_{n\in\mathbb{N}} A_n$, entonces $h(a)\neq h(a')$, porque f es inyectiva.

Si ambos pertenecen a $g[B]$, entonces $h(a)\neq h(a')$, porque g^{-1} es inyectiva.

El único caso interesante es si $a\in A_n$ y $a'\in g[B]$. Si $h(a)=h(a')$, entonces $f(a)=g^{-1}(a')$, o sea, $a'=g(f(a)\,)$, es decir, $a'\in A_{n+1}$, lo que es una contradicción. Luego $h(a)\neq h(a')$ en este caso también.

[4]Este teorema fue demostrado primero por Cantor en 1897, pero usando el Axioma de Elección. Schroeder propuso una prueba incompleta en 1898, corregida en 1911. Fue Bernstein quien en 1897 dio la primera prueba correcta y sin usar el Axioma de Elección.

Por último, veamos que h es sobreyectiva. Tomemos un $b \in B$. Si para todo $n \in \mathbb{N}$, $b \notin h[A_n] = f[A_n]$, entonces $b \in B - \bigcup_{n\in\mathbb{N}} f[A_n]$. Es claro por definición que $g(b) \notin A_0$, y si $g(b) \in A_{n+1} = g[f[A_n]]$, entonces $b \in f[A_n]$ contrario a nuestra elección de b. Hemos demostrado entonces que $g(b) \notin \bigcup_{n\in\mathbb{N}} A_n$. Por lo tanto, $h(g(b)) = g^{-1}(g(b)) \in B$, o sea b está en el recorrido de h, lo que completa la demostración de que h es sobreyectiva. □

Teorema 3.12. *El conjunto $\mathbb{R}$ de los números reales es equinumeroso con el conjunto $\mathcal{P}(\mathbb{N})$ de las partes del conjunto de los números naturales.*

Demostración. Demostraremos que el intervalo $[0,1]$ es equinumeroso con el conjunto $\mathcal{P}(\mathbb{N})$. Para ello expresemos los elementos de $[0,1]$ en su representación binaria, es decir,

$$a = 0, a_1\, a_2\, a_3 \cdots,$$

donde para cada $i \in \mathbb{N}$, $a_i \in \{0,1\}$. Aceptaremos aquí que todo real $a \in [0,1]$ tiene una única tal representación.

Definimos la siguiente función

$$\begin{aligned} f : [0,1] &\longrightarrow \mathcal{P}(\mathbb{N}) \\ a &\longmapsto \{i \in \mathbb{N} : a_i = 1\}. \end{aligned}$$

Es claro que para cada $a \in [0,1]$, $f(a) \subseteq \mathbb{N}$. Debemos demostrar que f es una biyección. Para ver que es inyectiva, si a, $b \in [0,1]$ y $a \neq b$, entonces para algún $m \in \mathbb{N}$, $a_m \neq b_m$. Entonces $m \in f(a)$ pero $m \notin f(b)$ o viceversa. Por lo tanto, $f(a) \neq f(b)$.

Para ver que f es sobreyectiva tomemos $A \subseteq \mathbb{N}$, y definamos $a \in [0,1]$ como sigue. El i–ésimo coeficiente de su expansión binaria verifica $a_i = 1$ si y sólo si $i \in A$. Es claro que a está bien definido. También es inmediato que $f(a) = A$. □

En el Teorema de Cantor–Schroeder–Bernstein se puede reemplazar funciones inyectivas por funciones sobreyectivas, sin embargo, este resultado requiere, una vez más, del Axioma de Elección. Lo mencionaremos en el próximo capítulo.

3.1.1 Cardinales infinitos. Los Alef

Vimos en la sección anterior que hay una infinidad de conjuntos con cardinalidades cada vez mayores: $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$, ... y los infinitos siguen creciendo.

Queremos ahora asignar una cardinalidad a los conjuntos infinitos. Definimos una sucesión $\aleph_0, \aleph_1, \aleph_2, \cdots$ (Lease alef cero, alef uno, ...)[5] de cardinalidades infinitas. El símbolo $\aleph_0$ corresponde a la menor cardinalidad infinita, la cardinalidad de $\mathbb{N}$ (y, por

[5]El símbolo $\aleph$ es la primera letra del alfabeto hebreo. Fue introducida por Cantor en 1895, según él, porque los símbolos de los otros alfabetos habían sido sobre utilizados. Además, estos conceptos nuevos requerían de representaciones nuevas.

lo tanto, de $\mathbb{Z}$, $\mathbb{Q}$ y todos los conjuntos equinumerosos con $\mathbb{N}$). $\aleph_1$ es la cardinalidad infinita que le sigue, etc.

Debe destacarse que no estamos afirmando que la cardinalidad de $\mathcal{P}(\mathbb{N})$ sea $\aleph_1$, la de $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ sea $\aleph_2$, etc., ¿cuál es la cardinalidad de $\mathcal{P}(\mathbb{N})$? Como vimos, $\mathcal{P}(\mathbb{N})$ es equinumeroso con $\mathbb{R}$ o "el continuo", por eso a ésta se le ha llamado la *cardinalidad del continuo*. Uno de los problemas más profundos de la teoría de conjuntos es establecer cuál es esta cardinalidad y durante años se intentó demostrar ya sea que la cardinalidad del continuo es $\aleph_1$ o que es distinta de $\aleph_1$.

La afirmación de que $\sharp\mathcal{P}(\mathbb{N}) = \aleph_1$ se conoce como la *Hipótesis del Continuo*. Cantor conjeturó que esta hipótesis era cierta. En los años 30 del siglo pasado, Kurt Gödel demostró que a partir de los otros axiomas de la teoría de conjuntos no se puede demostrar que la hipótesis fuese falsa. No fue sino hasta 1963 que P. Cohen demostró que tampoco se puede demostrar que sea verdadera. Quiere decir, entonces, que basados en nuestras intuiciones formalizadas por los axiomas, no se puede decidir cuál es la cardinalidad del continuo. El que no se pueda demostrar lo uno o lo otro no quiere decir que alguna de las dos afirmaciones no sea verdadera. De hecho, si la teoría de conjuntos es consistente, o sea no se desprende de ella una contradicción, entonces tiene que existir un modelo o universo en el que se verifican todos los axiomas. En éste, o bien la hipótesis del continuo es verdadera o bien es falsa.

Dado que la Hipótesis del Continuo es independiente de los otros axiomas, ella puede adoptarse como un nuevo axioma de la teoría. Basados en las consecuencias que este nuevo axioma tiene, actualmente la mayoría de los especialistas creen que la hipótesis es "falsa", en el sentido de que no es conveniente adoptarla como axioma para modelar la matemática según las intuiciones actuales.

3.1.2 Ejercicios

1. Si A es finito, encuentre la cardinalidad de $\mathcal{P}(A)$.
2. Demuestre que si $n < m$, no existe una biyección

$$f : \{0, 1, 2, \ldots, n\} \longrightarrow \{0, 1, 2, \ldots, n, n+1, \ldots, m\} .$$

3. Demuestre el Teorema 3.2.
4. Demuestre que hay infinitos números primos.
5. Demuestre que todos los círculos, de cualquier diámetro tienen el mismo número de puntos.
6. Demuestre que un cuadrado, (por ejemplo, $[0, 1] \times [0, 1]$) tiene la misma cantidad de puntos que un segmento (digamos, $[0, 1]$).
7. Demuestre que todo conjunto infinito contiene un subconjunto numerable.
8. Suponiendo el resultado anterior, demuestre que si a un conjunto infinito se le agrega un nuevo elemento, la cardinalidad no cambia, ¿qué pasa si se agrega una cantidad finita de elementos distintos?
9. Demuestre que un rectángulo tiene el mismo número de puntos que un cuadrado.
10. Demuestre que una esfera tiene tantos puntos como el plano.

11. Un número real se dice *algebraico* si es una raíz de un polinomio con coeficientes racionales. Por ejemplo, $\sqrt{2}$ es algebraico ya que es una raíz del polinomio $x^2 - 2$, pero π no es raíz de ningún polinomio con coeficientes racionales. (¡Esto es algo más difícil de demostrar!)

    Siguiendo los pasos que se indicarán a continuación, podrá demostrar que hay una cantidad numerable de números algebraicos.

    a) ¿Cuántas raíces puede tener un polinomio?
    b) ¿Cuántos polinomios con coeficientes racionales de primer grado hay?, ¿y de segundo grado?, ¿y de tercer grado? Más generalmente, ¿cuántos polinomios con coeficientes racionales de grado n hay?
    c) ¿Cuántas raíces de polinomios de grado n hay? Dicho de otro modo, ¿cuántos números algebraicos provienen de polinomios de grado n? Podemos definir el conjunto de todas las raíces de todos los polinomios de grado n.
    d) Observe que el conjunto de todos los números algebraicos es la unión de todos los conjuntos definidos en el punto anterior.
    e) Use el Teorema 3.6 para demostrar que hay una cantidad numerable de números algebraicos.

12. Los números reales que no son algebraicos, por ejemplo π y e, se llaman *trascendentes*, ¿cuántos números trascendentes hay?

Capítulo 4: Los Axiomas de Zermelo-Fraenkel

4.1 ¿Qué es una Teoría Axiomática?

En este capítulo daremos una idea de cómo se puede desarrollar una teoría axiomática que dé cuenta de las ideas más o menos intuitivas que hemos desarrollado en los capítulos anteriores.

En toda teoría axiomática debemos partir de términos que no podemos definir para no correr el riesgo de caer en un círculo vicioso. En la Teoría de Conjuntos estos son los conceptos de conjunto y pertenencia. Todas nuestras intuiciones descansan sobre la idea que tengamos sobre estos conceptos primitivos, sin embargo, para el desarrollo de la teoría no es imprescindible contar con estas intuiciones.

Una teoría axiomática es un modelo formal de una realidad que queremos estudiar. Está compuesta por *axiomas*, o sea, oraciones a partir de las cuales, usando sólo reglas lógicas, podamos obtener todas las propiedades de aquello que queremos modelar. Aunque los axiomas pueden ser totalmente arbitrarios, si el objetivo de la teoría es modelar una situación, los axiomas deben establecer las características y propiedades esenciales de los objetos que estamos tratando de describir en nuestro modelo. El ideal sería, en primer lugar, que los axiomas modelaran las intuiciones que tenemos de esa realidad y en segundo lugar, que la lista fuera completa, es decir, que todas y sólo aquellas propiedades de los objetos a describir se puedan obtener a partir de nuestra lista.

Diversas teorías axiomáticas de conjuntos han logrado en mayor o menor grado el primero de estos objetivos. El segundo, en cambio, obtener *todas* las propiedades de los conjuntos a partir de un sistema de axiomas, no se ha logrado. El motivo de esto es muy sencillo: no se puede. En efecto, los resultados obtenidos por el lógico Kurt Gödel alrededor de 1930, demuestran que es imposible dar una axiomatización completa de la Teoría de Conjuntos. Lo mismo es cierto de otras teorías matemáticas como la teoría de números.

Lo anterior parece condenar nuestro proyecto al fracaso, sin embargo, esto no es así, sólo nos advierte que el ideal es imposible. De hecho numerosos matemáticos han logrado establecer teorías axiomáticas que, si bien no completas, son suficientes para construir en ellas casi toda la matemática. En estas páginas hemos estudiado una de ellas, a saber, la teoría ZF, de Zermelo–Fraenkel, desarrollada a partir del trabajo de E. Zermelo, el primero en proponer una teoría formal y axiomática en su obra [**16**] de 1908. Esta axiomatización es la gran diferencia entre la teoría de conjuntos cantoriana, intuitiva y no formal, y la de Zermelo. Debe destacarse que la mayoría de los axiomas propuestos por Zermelo ya eran conocidos y usados por otros matemáticos. En [**2**] R.

Dedekind propone estos axiomas en una forma levemente distinta. Es, sin embargo, Zermelo el primero en plantear una teoría axiomática más o menos siguiendo el estilo de los Elementos de Euclides. La teoría que presentamos es una versión moderna y difiere algo de la propuesta por Zermelo.

Como vimos en el primer capítulo, la idea intuitiva de que a cada propiedad o predicado imaginable le corresponde un conjunto, no es adecuada porque surgen contradicciones. La paradoja de Russell (y otras) nos dice que el concepto de "propiedad" es más delicado de lo que suponemos y que definitivamente no debe corresponder a lo que llamamos un conjunto. Debemos tomar medidas para evitar que esta paradoja y ninguna otra se produzca en nuestra teoría.

Sin embargo, la noción de que a cada propiedad debería corresponder la colección de objetos que la verifican, lo que habitualmente llamamos la "extensión" de la propiedad, tiene fuerte arraigo en nuestra intuición. Algunos matemáticos no han querido deshacerse de ella y han elaborado teorías bastante complejas, que incluyen dos tipos de objetos, conjuntos y *clases* . Estas últimas corresponden a las extensiones de propiedades y son los objetos primitivos de la teoría. En estas teorías los conjuntos se definen como aquellas clases que pertenecen a otra clase, aquellas clases que no pertenecen a otra clase se denominan *clases propias*. Es decir, las clases propias son las extensiones de una propiedad que de alguna manera son "demasiado grandes": no las podemos aprehender porque no pertenecen a ninguna clase mayor. Ejemplos de estas últimas son la clase de Russell R , definida anteriormente en el Capítulo 1, o la clase V formada por todos los conjuntos (o clase universal). El lector puede consultar [**13**] y [**10**] para aprender sobre estas teorías. Lo cierto es que la abrumadora mayoría de los trabajos en fundamentos de la matemática se enmarcan en la teoría ZF.

La noción de propiedad o predicado no la hemos definido pero de lo anterior se desprende que es central en nuestro estudio. Como queremos mantener este estudio dentro de los márgenes de una teoría, sin el rigor extremo de la lógica matemática, daremos aquí una descripción intuitiva. En el Apéndice B al final de este capítulo puede encontrarse una versión más formal.

Lo que queremos evitar son definiciones de conceptos vagos o inaplicables. Por ejemplo, nos damos cuenta de que el "conjunto de los números enteros que son azules", es un concepto totalmente irrelevante para la matemática. A su vez, el "conjunto de los números terminados en 4", si bien tiene contenido matemático no resulta muy útil, porque es ambiguo, depende del sistema de notación (decimal, binario, etc.) Nos limitaremos entonces a expresiones que se pueden escribir en forma precisa a partir del mínimo de conceptos. Como nuestros únicos conceptos primitivos son los conjuntos y la noción de pertenencia, en principio, sólo usaremos esos, además de los conceptos lógicos habituales como conjunciones, disyunciones y negaciones. Naturalmente, para que el resultado sea legible, en la definición de nuevas propiedades también aceptamos conceptos que ya hemos definido previamente a partir de los conceptos primitivos, por ejemplo, conjunto vacío, uniones, intersecciones, etc. Sólo son aceptables y representan propiedades en nuestra teoría, aquellas que sean definidas de esta manera.

4.2 Los Axiomas de Zermelo-Fraenkel I

Veremos aquí someramente los axiomas elementales mencionados en el Capítulo 1 y que sirven para desarrollar la teoría elemental.

A1. Axioma de Extensionalidad:
"Si todo elemento de X es un elemento de Y y todo elemento de Y es un elemento de X, entonces X es igual a Y."

Dicho de otro modo, si dos conjuntos tienen los mismos elementos, entonces son iguales. Probablemente este es el axioma más sencillo pero es bastante profundo, nos dice que lo que caracteriza a un conjunto son sus elementos.

Note que la implicación recíproca, a saber, "si X es igual a Y entonces todo elemento de X es un elemento de Y y todo elemento de Y es un elemento de X" es sólo una característica de la identidad. Dos conjuntos iguales satisfacen las mismas proposiciones, en particular, tienen los mismos elementos.

A2. Axioma de Separación:
"Dados un conjunto X y una propiedad cualquiera, existe un conjunto Y cuyos elementos son aquellos elementos de X que verifican esa propiedad"

Este axioma nos dice que para cualquier propiedad simbolizada por P y cualquier conjunto X existe el subconjunto $\{x \in X : x$ verifica la propiedad $P\}$ de X, formado por los elementos que verifican esa propiedad. Este conjunto es único en virtud del axioma **A1**.

Cabe destacar que éste no es propiamente un axioma sino más bien un *esquema de axiomas*, que produce muchos axiomas. En efecto, para cada propiedad P tenemos un axioma distinto, o sea, hay una cantidad ilimitada de instancias de este axioma.

Como mencionamos en el Capítulo 1, este axioma, a veces conocido como el axioma de Zermelo, es el que impide que se produzcan las paradojas del tipo de la de Russell y otras paradojas, las llamadas semánticas, cuyo origen está en aplicar a los conjuntos propiedades que no tienen sentido. Dedekind y Cantor no percibieron la necesidad de este axioma, pero claro, sus trabajos son anteriores a la paradoja de Russell.

Teorema 4.1. *No existe el conjunto de todos los conjuntos.*

Demostración.
Supongamos que sí existe y llamémoslo V. Entonces, en virtud del axioma **A2**, podemos construir el conjunto de Russell $R = \{x \in V : x \notin x\}$. Se produce entonces la misma contradicción que vimos antes en el Capítulo 1.

□

A3. Axioma del Conjunto Vacío:

"Existe un conjunto que no contiene ningún elemento."

Observemos que, en particular, este axioma garantiza que existe al menos un conjunto.

Como demostramos en el capítulo 1, existe un único conjunto que no contiene ningún elemento, lo que nos autoriza a llamarlo *el* conjunto vacío y denotarlo $\emptyset$.

Este axioma puede ser reemplazado por otro que dice

A3'. "Existe por lo menos un conjunto".

Usando esta proposición y el axioma **A2** obtenemos el axioma **A3.** Para ello, llamemos C al conjunto que la proposición dice que existe y formemos su subconjunto

$$\{x \in C : x \neq x\}.$$

Es fácil ver que este conjunto no tiene elementos, luego por el axioma **A1**, es el conjunto vacío. Por su parte, el axioma **A3** obviamente implica la proposición **A3',** por lo tanto, en presencia de los otros axiomas, son equivalentes. Puede entonces reemplazarse el axioma **A3** por la proposición **A3'.**

Si bien hoy el conjunto vacío es algo totalmente natural, despertó un enorme rechazo entre los matemáticos de la época de Cantor. Dado que los conjuntos quedan definidos por sus elementos, para ellos era inconcebible que existiera un conjunto que no tiene elementos. En el Capítulo 1 hicimos notar cuán útil es contar con este concepto.

A4. Axioma de Pares:

"Dados dos conjuntos X e Y, existe un conjunto cuyos únicos elementos son X e Y."

Resulta claro por el axioma **A1** que este conjunto es único. Este axioma es muy intuitivo y no merece mayor análisis, sin embargo, también despertó recelo en los orígenes de la teoría. El motivo de éste es que se pensaba los conjuntos como "pluralidades". Ahora bien, una consecuencia de este axioma es que si $X = Y$, entonces tenemos el conjunto $\{X\}$, con un único elemento. ¿Cómo puede haber una pluralidad singular? Como vemos, se trata de un problema semántico derivado de no tener un concepto abstracto claro de qué es un conjunto y usar en su lugar nociones intuitivas, como pluralidad, agregado y otras.

A5. Axioma de Uniones:

"Si X es un conjunto, entonces existe un conjunto que contiene a todo aquel conjunto que pertenece a alguno de los elementos de X."

Nuevamente por axioma **A1**, este conjunto es único, se llama la *unión* de X y como vimos se le denota $\bigcup X$. También vimos en el Capítulo 1 que la unión de dos conjuntos es un caso particular de las construcciones que se pueden hacer con el axioma **A4**.

A6. Axioma del Conjunto Potencia:

"Si X es un conjunto, entonces existe el conjunto de todos los subconjuntos de X".

Para cada X este conjunto es único y lo llamamos el *conjunto potencia* de X. La pertinencia de este axioma es también evidente. Una de las importancias de esta construcción es que permite tener conjuntos más y más grandes, en particular, de cardinalidades tan grandes como queramos.

4.3 Los Axiomas de Zermelo-Fraenkel II

En esta sección estudiamos los axiomas más complejos de ZF. Estos se necesitan para obtener operaciones más difíciles sobre conjuntos de modo que podamos construir más conjuntos a partir de los elementales.

A7. Axioma del Conjunto Infinito:

El nombre de este axioma es un poco engañoso, la verdad es que el axioma no dice literalmente "*Existe un conjunto que tiene infinitos elementos*" como uno podría esperar, sino que garantiza la existencia de un conjunto que intuitivamente tiene que ser infinito. Si como antes llamamos sucesor de un conjunto x al conjunto $x \cup \{x\}$, entonces el axioma dice:

"Existe un conjunto que contiene al conjunto vacío y que contiene al sucesor de cada uno de sus elementos."

Intuitivamente el conjunto así formado es infinito, ya que para cada conjunto $y \in X$ hay otro y otro y otro, todos ellos diferentes. Como vimos en el capítulo 2, los conjuntos que verifican las condiciones indicadas en este axioma se llaman inductivos. Quizás un nombre más adecuado para este axioma sería "Axioma del Conjunto Inductivo", pero la costumbre manda. El axioma nos dice que existe al menos un conjunto inductivo y, como vimos en el Capítulo 2, es necesario para construir el conjunto de los números naturales como el menor de los conjuntos inductivos.

Este axioma representa un profundo quiebre con la tradición filosófica. Hasta mediados del siglo XIX, siguiendo el pensamiento griego, los matemáticos consideraban el infinito como algo potencial, es decir, procesos que se pueden continuar y continuar sin fin. Por ejemplo, dado un número natural, siempre podemos obtener otro y otro y otro. Sin embargo, la noción de un objeto infinito como un todo no era concebible. Lo que hicieron los lógicos matemáticos de ese tiempo, entonces, fue afirmar que hay conjuntos que son realmente y no sólo potencialmente infinitos. Por supuesto esta no es una idea de Zermelo, sino que está en el centro del pensamiento de Cantor. En la literatura suele llamarse infinito potencial e infinito actual a estas dos formas de considerar el infinito. Para más información sobre este tema ver [**13**].

El axioma original de Zermelo era algo distinto, decía

"Existe un conjunto que contiene al conjunto vacío y si x es uno de sus elementos también lo es $\{x\}$".

La versión actual se debe a John von Neumann.

A8. Axioma de Reemplazo:

Para introducir el siguiente axioma de ZF, debemos estudiar antes un cierto tipo de propiedades que relacionan pares de conjuntos.

Una propiedad o predicado binario $P(x, y)$, es decir, que se refiere a dos variables es una *función proposicional* si para todo conjunto a existe un único conjunto b tal que $P(a, b)$ se verifica. Ejemplos de éstas propiedades $P(x, y)$ son las siguientes:

$$y = \bigcup x\,, \quad y = \mathcal{P}(x)\,, \quad y = x \cup \{x\}\,, \quad y = x \cap a\,.$$

Vemos que para cada conjunto a existe un único conjunto que verifica la propiedad. Una definición formal de función proposicional aparece en el Apéndice B.

El axioma de reemplazo dice:

"Si $P(x, y)$ es una función proposicional y A es un conjunto, entonces existe el conjunto de los elementos b que verifican $P(a, b)$ para algún $a \in A$".

Usando las notaciones habituales, el conjunto garantizado por este axioma es

$$\{b \,:\, P(a, b) \quad \text{para algún} \quad a \in A\}\,.$$

Este axioma parece más complicado de lo que es. La idea intuitiva es que si a cada elemento a de un conjunto A podemos asociar un único conjunto que denotamos b_a, entonces existe un conjunto formado por los elementos b_a.

Observemos que estamos hablando de algo muy parecido a una función. En efecto, si a cada conjunto x asociamos

$$x \longmapsto \text{ el único } y \text{ tal que } P(x, y)\,,$$

esta no es una función porque, para serlo debería ser subconjunto del producto cartesiano $B \times C$ de dos conjuntos. Esto no es así, porque esta "función" está definida para todo conjunto, es decir, su dominio sería el conjunto de todos los conjuntos que, como vimos, no existe dentro de nuestra teoría. Sin embargo, cuando restringimos dicho "dominio" a un conjunto A, el axioma **A8** garantiza que existe el recorrido de la "función".

Una intuición detrás de este axioma es que en esta construcción se agrega un elemento por cada elemento de A, por lo que se obtienen conjuntos que son a lo más, tan grandes como el original.

El axioma de reemplazo fue propuesto por Fraenkel en 1922 y es su contribución a la teoría ya desarrollada por Zermelo. La formulación que hemos dado es la estándar actualmente, fue propuesta independientemente por T. Skolem más o menos al mismo tiempo que Fraenkel, sin embargo, es el nombre de este último el que ha quedado ligado al axioma. Incluso antes, en 1917, una forma particular de este axioma fue propuesta por Mirimanoff.

El problema que originó el Axioma de Reemplazo es el descubrimiento de que no se puede probar en la teoría de Zermelo que

$$\{\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})), \dots\}$$

sea un conjunto. El Axioma de Reemplazo no tiene gran relevancia en la teoría de conjuntos elemental, pero es imprescindible para la definición de números ordinales, una generalización de los números naturales, que representan a todos los buenos órdenes posibles. Si bien no estudiaremos este tema en este libro, es una de las motivaciones del desarrollo de la teoría de conjuntos desde Cantor en adelante.

A9. Axioma de Regularidad:

El axioma de regularidad no ha sido usado en este libro porque no se requiere para los propósitos que nos hemos planteado. Como veremos a continuación en el Teorema 4.2 este axioma impide la existencia de un conjunto a tal que $a \in a$ o que $a \in b \in a$ o que $a \in c \in b \in a$, etc. Dado que los conjuntos quedan definidos por sus elementos y estos a su vez están definidos por sus elementos, los conjuntos que queramos definir no pueden contenerse a sí mismos, ni sus elementos pueden contenerlo, ni los elementos de sus elementos pueden contenerlo, etc. Por ejemplo, si un conjunto dado a fuera tal que $a \in a$, para definirlo necesitaríamos haber establecido antes la existencia de sus elementos, en particular, de a mismo, lo que es absurdo. El propósito de este axioma es entonces impedir las definiciones circulares.

El axioma dice:

"Todo conjunto no vacío contiene un elemento con el que no comparte ningún elemento."

Una manera más operativa de leer este axioma es que para cada conjunto no vacío A, existe un elemento $a \in A$ tal que $a \cap A = \emptyset$. Obsérvese que en caso contrario, A compartiría un elemento con cada uno de sus subconjuntos.

Teorema 4.2.

1. *Para todo conjunto* a, $a \notin a$.
2. *Dados dos conjuntos* a *y* b, *o bien* $a \notin b$ *o bien* $b \notin a$.
3. *En general, no existen* $a_1, a_2, \dots, a_n$ *tales que* $a_1 \in a_2 \in \cdots \in a_n \in a_1$.

Demostración.

1. Supongamos que existe a tal que $a \in a$, entonces $A = \{a\}$ contradice al axioma **A9**.
2. Idem 1, con $A = \{a, b\}$.
3. Idem 1, con $A = \{a_1, a_2, \dots, a_n\}$.

□

En Teorema 2.18 del Capítulo 3 usamos precisamente este resultado para ver propiedades del orden de los números naturales. Sin embargo, en el caso de los números naturales no fue necesario usar este axioma. La inclusión del Axioma de Regularidad se justifica para garantizar ese resultado a todo conjunto.

Hay una consecuencia mucho más sutil del Axioma de Regularidad. En el siguiente teorema demostramos que los conjuntos no pueden tener "profundidad" infinita, es decir, si miramos en los elementos de los elementos de los elementos, etc., de un conjunto, tarde o temprano llegamos "al fondo", al conjunto vacío.

Teorema 4.3. *No existen conjuntos* $a_1, a_2, a_3, \ldots, a_n, \ldots$ *tales que*

$$\cdots \in a_n \in \cdots \in a_3 \in a_2 \in a_1.$$

(Esta última expresión es una abreviación de las afirmaciones $x_{i+1} \in x_i$*).*

Demostración. Por hipótesis, para cada $n \in \mathbb{N}$ hay un (único) a_n asociado, de modo que tenemos una función cuyo dominio es $\mathbb{N}$. El axioma **A8** garantiza que el conjunto

$$A = \{a_n : n \in \mathbb{N}\}$$

existe. Entonces, A contradice al axioma **A9** ya que para cualquier $y \in A$, digamos $y = a_m$ para algún m, $a_{m+1} \in a_m$ y $a_{m+1} \in X$, o sea $y \cap X \neq \emptyset$. □

Ejercicio 4.4. En el capítulo 2 vimos que el conjunto $\mathbb{N}$ de los números naturales contiene al 0, $S0$, $S(S0)$, etc. Lo que no es tan claro es que los contenga sólo a ellos y nada más. Esto es lo que veremos a continuación usando el Axioma de Regularidad.

Lema 4.5. *Todo número natural distinto de 0 se puede obtener a partir de 0 reiterando la operación sucesor.*

Demostración. Sea $x \in \mathbb{N}$. Como $x \neq 0$ tenemos $x = Sx_1$, para algún número natural x_1 y en particular, $x_1 \in x$. Además $x_1 \neq x$, por que en caso contrario tendríamos $x \in x$, lo que como vimos es imposible. Similarmente, si $x_1 \neq 0$, entonces $x_1 = Sx_2$, con $x_2 \in x_1$. El proceso puede continuar obteniéndose

$$\cdots x_m \in x_{m-1} \in \cdots \in x_2 \in x_1 \in x\,.$$

Consideremos entonces el conjunto $A = \{y \in \mathbb{N} : y \in x\}$. Vemos que por el Lema 2.10, A contiene a todos los elementos de la $\in$–cadena generada anteriormente. Pero hemos visto en el Teorema 4.3 que esto no es posible. Por lo tanto, este proceso debe detenerse en algún momento, es decir, hay algún m tal que $x_m = \emptyset = 0$.

Ahora es fácil ver por la manera en la que se obtuvo cada x_i que x es el sucesor del sucesor del sucesor... (m veces) de 0. □

Existen teorías de conjunto que limitan el Axioma de Regularidad a los casos finitos descritos en el Teorema 4.2. El Axioma de Regularidad no estaba en la lista original de Zermelo y es probable que fuera propuesto por von Neumann. En cualquier caso, fue adoptado o propuesto independientemente por el propio Zermelo en 1930. La forma del axioma original es nuestro Teorema 4.3.

Esta lista de nueve axiomas conforman ZF. Junto con el Axioma de Elección que estudiaremos en la próxima sección, son suficientes para desarrollar casi toda la matemática. Inmediatamente se nos ocurren varias preguntas: ¿son estos axiomas independientes entre sí?, ¿o es que pueden obtenerse unos de otros? La respuesta a esta última interrogante es sí, el axioma de pares puede obtenerse a partir de los axiomas de reemplazo y del conjunto potencia. Por su parte, el axioma del conjunto vacío puede obtenerse a partir del axioma de separación y del axioma del conjunto infinito (habría que darle otra formulación a este último).

Más importante aún es el problema de la consistencia, es decir, ¿es posible deducir una contradicción a partir de estos axiomas? Por supuesto no se ha descubierto ninguna contradicción, de no ser así, no tendría sentido el estudio de esta teoría, y se actúa como si fueran consistentes.

Este problema no se ha resuelto y no parece probable que vaya a resolverse debido a los resultados de Gödel en 1930. En ellos se demuestra que la consistencia de la teoría de conjuntos sólo podría ser probada dentro de una teoría al menos tan poderosa como la propia teoría de conjuntos, de modo que la pregunta sobre la consistencia no tiene respuesta.

Dado que la consistencia de ZF no es demostrable, los matemáticos se dedicaron a obtener resultados llamados de consistencia relativa, es decir, suponiendo que ZF es consistente, entonces sucede tal o cual cosa. En un trabajo de 1940 Gödel demuestra la consistencia relativa del axioma de elección. En 1963, Paul Cohen demostró la consistencia relativa de la negación del Axioma de Elección. Estos resultados prueban que este Axioma es independiente de los otros axiomas.

El otro problema que surge naturalmente es el de la completud de este sistema de axiomas. Es decir, ¿son suficientes éstos para deducir todos los teoremas posibles sobre conjuntos? La respuesta también es negativa. Mas aún, sabemos, nuevamente en virtud de los trabajos de K. Gödel en 1930, que no puede completarse, es decir, aunque agreguemos una lista de infinitos axiomas a ZF, la nueva teoría seguirá siendo incompleta, es decir, siempre existirá una oración φ tal que ni ella ni su negación puede demostrarse a partir de esa lista de axiomas. Sin embargo, es claro que una de estas dos oraciones debe ser cierta. Todos estos problemas requieren de conocimientos de Lógica Matemática y están fuera del alcance de esta obra. Nos parece interesante, eso sí, mencionarlos para que el lector investigue por su cuenta. Un libro de fácil acceso para este propósito es [**13**].

4.3.1 Ejercicios

1. En rigor, para definir $x \cap y$ no necesitamos axioma **A4**, ¿cómo podríamos hacerlo?
2. Demuestre que el axioma de pares puede ser reemplazado por el axioma más débil:

   "Dados dos conjuntos X e Y, existe un conjunto que los contiene a ambos".

   Esto quiere decir que el axioma de pares se puede deducir de este axioma (junto a los otros axiomas de la teoría) y recíprocamente, este axioma se deduce del de pares.
3. Demuestre que el axioma de uniones puede ser reemplazado por el axioma más débil:

   "Si X es un conjunto, entonces existe un conjunto que contiene a todos los elementos de los elementos de X".
4. Demuestre que el axioma del conjunto potencia puede ser reemplazado por el axioma más débil:

   "Si X es un conjunto, entonces existe un conjunto que contiene a todos los subconjuntos de X".
5. Demuestre que el Axioma de Pares puede obtenerse a partir de los axiomas de Reemplazo y del Conjunto Potencia.
6. Demuestre el Axioma del Conjunto Vacío a partir de los otros axiomas y el nuevo axioma: "Existe un conjunto infinito".
7. Use el Axioma de Regularidad para demostrar que si $Sx = x \cup \{x\}$ como en la definición de sucesor de un número natural dada en el capítulo 2, entonces $Sx = Sy$ implica $x = y$.

4.4 El Axioma de Elección

En la formulación original de su Teoría de Conjuntos, en 1908, Zermelo incluye otro axioma, el Axioma de Elección. Más tarde lo dejó explícitamente fuera de su axiomatización porque lo consideraba de una naturaleza distinta de los otros, debido a su carácter no constructivo y a las importantes, a veces sorprendentes, consecuencias que de él se desprenden. Por otra parte, para todo efecto práctico éste siempre era considerado como un axioma más. A menudo nos referimos a la teoría ZFC[1], cuando incluimos el axioma de elección.

El Axioma de Elección puede ser presentado en muchas formas. Estudiaremos varias formulaciones diferentes y enseguida algunas de sus aplicaciones.

Como veremos, una de las formulaciones equivalentes del Axioma es que todo conjunto puede bien ordenarse. Cantor lo propuso como una regla lógica más, sin embargo, a sus contemporáneos no les pareció en absoluto evidente este nuevo principio. Es en la solución de este problema en [**15**] que Zermelo hizo uso del Axioma de Elección. Esta proposición era usada con anterioridad, pero nadie reparaba en que se trataba de un principio totalmente distinto que requería, si no de una justificación, al menos de una mención. Por lo tanto, la importancia de Zermelo en este caso fue poner de manifiesto que aquí había un principio matemático nuevo que aparentemente

[1] La C tiene su origen en el nombre inglés del axioma: Axiom of Choice.

no se desprendía de los otros y que permitía postular la existencia de conjuntos sin construirlos.

La demostración del Principio del Buen Orden en [**15**] despertó muchas críticas, es por eso que Zermelo se convenció que debía trabajar en un sistema axiomático que fuera inmune a esas objeciones. El resultado fue la primera axiomatización de la teoría de conjuntos en [**16**]. La formulación del Axioma de Elección que aparece en ese trabajo es levemente distinta de la que entregamos aquí.

Axioma de Elección (AC):

"Si A es un conjunto cuyos elementos son conjuntos no vacíos, entonces existe una función F cuyo dominio es A y tal que para todo $x \in A$, $F(x) \in x$ ".

Tal función se llama una *función de elección para* A.

Observemos que

$$\begin{aligned} F : A &\longrightarrow \bigcup A \\ x &\longmapsto F(x) \in x \end{aligned}$$

La existencia de una función de elección implica elegir simultáneamente un elemento de cada conjunto que pertenece a A. Esto no representa ningún problema si A es finito, sin embargo, si A es infinito, no es en absoluto intuitivo que se pueda hacer. Nótese también que el axioma no da ninguna idea de cómo construir tal función. Esto es esencial en este axioma, si existe un algoritmo o método para elegir el elemento, entonces el axioma no es necesario. Bertrand Russell dio un muy buen ejemplo de este fenómeno. Supongamos que tenemos un conjunto infinito C de pares de calcetines y un conjunto infinito Z de pares de Zapatos. Nos piden elegir un calcetín de cada par y, análogamente, escoger un zapato de cada par. Para el primer problema necesito usar el Axioma de Elección. Para el segundo no es necesario porque puedo, por ejemplo, escoger siempre el zapato izquierdo.

En un ejemplo más matemático, si el conjunto A está formado por conjuntos no vacíos de números naturales, entonces no necesitamos usar el axioma de elección, ya que como los naturales están bien ordenados, para cada $a \in A$ podemos elegir su menor elemento.

4.4.1 Equivalencias del Axioma de Elección

La siguiente es una lista de los principios más importantes que son equivalentes al axioma de elección.

Principio de Buen Orden:

"Todo conjunto puede bien ordenarse".

Ya hemos mencionado este principio varias veces. Dentro de la teoría es considerado un teorema ya que es consecuencia del Axioma de Elección. Desde que fue propuesto por Cantor despertó sospechas entre los matemáticos por su naturaleza no

constructiva. Como vimos, Zermelo puso de manifiesto el uso del Axioma de Elección para justificar este principio. Por supuesto, el axioma igualmente no es constructivo, sin embargo, parece ser mucho menos intuitivo.

Lema de Zorn:

> *"Si A es un conjunto parcialmente ordenado por R y todo subconjunto de A totalmente ordenado por R tiene una cota superior en A, entonces A tiene un elemento maximal".*

Un subconjunto de A totalmente ordenado por R se llama una *R-cadena.*
El Lema de Zorn es probablemente la forma más usual de aplicación del Axioma de Elección. Forma parte de una serie de principios, llamados principios maximales, todos similares en su formulación, que fueron descubiertos y redescubiertos por distintos autores en las primeras tres décadas del siglo XX, entre ellos Hausdorff y Kuratowski.

La versión hoy conocida como Lema de Zorn fue propuesta por Max Zorn en 1935, aunque una versión preliminar ya aparece en los trabajos de Kuratowski en 1922. Zorn lo planteó como un nuevo axioma que reemplazara al Teorema del Buen Orden en sus usos en álgebra. Este último era la forma del Axioma de Elección usada por los algebristas en esa época. La forma que hemos presentado aquí es la más usada actualmente, la propuesta por Zorn se refería sólo al orden parcial de ser subconjunto.

Los siguientes dos principios, si bien no tan relevantes como los anteriores, son muy importantes en la teoría de cardinalidades. Ellos nos permiten, entre otras cosas, probar que las cardinalidades de los conjuntos verifican la ley de tricotomía. Ambos son equivalentes al Axioma de Elección.

Principio de Tricotomía:

> *"Dados dos conjuntos A y B, existe una función inyectiva de A en B o existe una función inyectiva de B en A".*

Principio de la Imagen Inversa:

> *"Dados dos conjuntos no vacíos A y B, existe una función sobreyectiva de A en B o existe una función sobreyectiva de B en A.".*

Teorema 4.6. *Todos los principios anteriores son equivalentes al axioma de elección.*

Demostración. La demostración de este teorema es bastante compleja. La incluimos en el Apéndice A. □

4.4.2 Aplicaciones

En todas las ramas de las matemáticas hay importantes aplicaciones del axioma de elección. A continuación daremos una breve lista con algunas de éstas.

1. Todo espacio vectorial tiene una base.
2. La unión enumerable de conjuntos enumerables es enumerable.
3. Todo anillo con unidad tiene un ideal maximal.
4. Todo orden parcial puede extenderse a un orden total.
5. Todo cuerpo tiene una clausura algebraica.

Demostraremos algunas de éstas. Supondremos que el lector maneja los conceptos involucrados en cada caso.

Teorema 4.7. *Todo espacio vectorial tiene una base.*

Demostración.
Sea V un espacio vectorial y sea $A = \{B \subseteq V : B$ es linealmente independiente$\}$ parcialmente ordenado por inclusión.

Sea entonces $C = \{B_i : i \in I\}$ una cadena de elementos de A. Entonces, $\bigcup C \subseteq V$ y $\bigcup C$ contiene a todos los miembros de la cadena.

Veremos ahora que $\bigcup C$ es linealmente independiente.

Sean $v_1, v_2, \ldots, v_n \in \bigcup C$. Entonces existe $B_1, \ldots, B_n \in C$ tales que $v_i \in B_i$, $i \leq n$. Pero C es una cadena, luego $B_i \subseteq B_n$, $i \leq n$, por lo tanto, $v_1, \ldots, v_n \in B_n$ y, por consiguiente, son linealmente independientes. Esto demuestra que $\bigcup C$ es un conjunto linealmente independiente.

Por lo tanto, $\bigcup C$ pertenece a A, luego toda cadena de A tiene una cota superior y por el lema de Zorn A tiene un elemento maximal.

Probar que un conjunto linealmente independiente maximal es una base, es un ejercicio elemental de algebra lineal.

□

Teorema 4.8. *La unión enumerable de conjuntos enumerables es enumerable.*

Demostración. Como hicimos notar en el Capítulo 3, hay un uso encubierto del axioma de elección en la demostración que allí dimos de este teorema. Daremos ahora los detalles de esa demostración.

Sea $C = \{C_i : i \in \mathbb{N}\}$ un conjunto enumerable de conjuntos enumerables.

Eso quiere decir que existe para cada C_i una biyección entre C_i y $\mathbb{N}$. El problema es que no hay una sino muchas, en general, infinitas y debo elegir una de ellas. Si hubiera una cantidad finita de conjuntos C_i, no habría problema. Éste se suscita cuando tenemos que elegir simultáneamente una biyección para cada uno de los infinitos C_i.

Sean $K_i = \{f : \mathbb{N} \longrightarrow C_i : f$ es una una biyección$\}$ y $K = \{K_i : i \in \mathbb{N}\}$. Entonces K es un conjunto de conjuntos no vacíos por lo tanto hay una función de

elección

$$\begin{aligned} F : K &\longrightarrow \bigcup K \\ K_i &\longmapsto f_i \in K_i \end{aligned}$$

es decir, para cada $i \in \mathbb{N}$, $f_i : \mathbb{N} \longrightarrow C_i$ es una biyección, que es lo que necesitábamos. □

Teorema 4.9. Principio de Extensión de Órdenes:

Todo orden parcial puede extenderse a un orden total maximal.

En otras palabras, si R es un orden parcial, entonces hay un orden total M tal que $R \subseteq M$. Es decir, si xRy entonces xMy.

Este resultado es bastante sorprendente, nos dice que cualquier orden puede pensarse como una vista limitada de algún orden total. Piense, por ejemplo, el lector, en todos los subconjuntos de los números naturales ordenados por inclusión ($\subseteq$). Estos pueden reordenarse de tal manera que todos sean comparables unos con otros, pero respetando las inclusiones. Naturalmente hay muchas maneras de extender un orden parcial para que sea total.

Este teorema fue demostrado en 1930 por el matemático polaco E. Szpilrjan usando el principio maximal de Kuratowski, una versión anterior del Lema de Zorn.

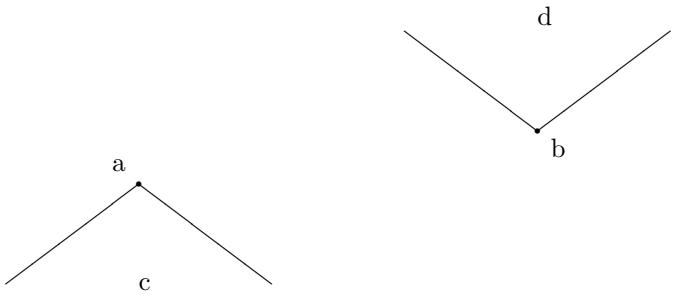
Demostración. Sean $R \subseteq A \times A$ un orden parcial y sea

$$A = \{T \in \mathcal{P}(A \times A) \,:\, R \subseteq T \text{ y } T \text{ es un orden }\}.$$

Consideramos A ordenado por inclusión. Entonces, toda cadena B tiene una cota superior, a saber, $\bigcup B$. Por el Lema de Zorn, A tiene un elemento maximal, llamémoslo M. Es claro que M es un orden parcial que contiene a R. Tenemos que verificar que M es un orden total.

Para una demostración por contradicción, supongamos que existen dos conjuntos a y $b \in A$ tales que $a \neq b$, $(a, b) \notin M$ y $(b, a) \notin M$. Lo que haremos es extender el orden M a un orden M' tal que $(a, b) \in M'$. Usaremos las notaciones $x \leq_M y$ y $x \leq_{M'} y$ para denotar estas relaciones de una manera más natural. Haremos una construcción que puede parecer complicada, sin embargo, tiene una base muy intuitiva.

El diagrama siguiente nos muestra una vista parcial del orden M. Los conjuntos a y b no están relacionados, pero como en el nuevo orden sí lo están, todo conjunto $c \leq_M a$ deberá ser menor que b. Más aún, para preservar la transitividad, c deberá ser menor que todo d tal que $b \leq_M d$. Sucede que con eso basta.



Definimos

$$M' = M \cup \{(c,d) \,:\, c \leq_M a \;\text{ y }\; b \leq_M d\}\,.$$

Ésta es una relación obviamente reflexiva, ya que no hemos agregado elementos nuevos, que no aparecieran en M, y esta última es una relación reflexiva.

Para verificar la antisimetría, consideremos pares (c,d) tales que $c \leq_{M'} d$ y $d \leq_{M'} c$. Hay cuatro casos.
Caso 1. $c \leq_M d$ y $d \leq_M c$. Entonces $c = d$ porque M es antisimétrica.
Caso 2. $c \leq_M d$ y $d \leq_{M'} c$. En este caso tenemos $d \leq_M a$ y $b \leq_M c$ y, por lo tanto,

$$b \leq_M c \leq_M d \leq_M a\,,$$

y por la transitividad de M, tendríamos que $b \leq_M a$, lo que es contrario a nuestra hipótesis.
Caso 3. $c \leq_{M'} d$ y $d \leq_M c$. Este caso es similar al anterior.
Caso 4. $c \leq_{M'} d$ y $d \leq_{M'} c$. En este caso tenemos $c \leq_M a$ y $b \leq_M d$ y también $d \leq_M a$ y $b \leq_M c$, lo que nuevamente contradice nuestra hipótesis.

Vemos que sólo el primer caso es posible y, por lo tanto, se verifica la antisimetría de M'.

Para verificar la transitividad de M', supongamos que $c \leq_{M'} d$ y $d \leq_{M'} e$. Nuevamente hay cuatro casos.
Caso 1. $c \leq_M d$ y $d \leq_M e$. Entonces $c \leq_M e$ porque M es transitiva.
Caso 2. $c \leq_M d$ y $d \leq_{M'} e$. En este caso tenemos $d \leq_M a$ y $b \leq_M e$ y, por lo tanto,

$$c \leq_M d \leq_M a\,,$$

y por la transitividad de M, tendríamos que $c \leq_M a$. Esto último unido a que $b \leq_M e$, nos dice que $c \leq_{M'} e$.
Caso 3. $c \leq_{M'} d$ y $d \leq_M e$. Este caso es similar al anterior.

Caso 4. $c \leq_{M'} d$ y $d \leq_{M'} e$. En este caso tenemos $c \leq_M a$ y $b \leq_M d$ y también $d \leq_M a$ y $b \leq_M e$. Vemos que en particular, $c \leq_M a$ y $b \leq_M e$, es decir, $c \leq_{M'} e$.

En cualquier caso se verifica la transitividad de M'.

Lo que hemos demostrado es que si M no es un orden total, entonces puede extenderse a un orden más grande que también contiene a R, lo que contradice el que M sea maximal. □

La demostración anterior nos ilustra también dónde podrían estar las multiples elecciones arbitrarias. Vemos que para cada par (a, b) de conjuntos no relacionados según R podemos agregar uno de los dos, cualquiera. Esto obliga a incluir a otra gran cantidad de pares. Este proceso debe ser continuado una y otra vez hasta que se logre un orden total. Es fácil imaginarse un ejemplo en el que hay una cantidad infinita de estas elecciones arbitrarias.

En matemáticas avanzadas hay importantes aplicaciones del Axioma de Elección en alguna de sus formas. Por ejemplo,

- existe un conjunto de números reales que no es Lebesgue-medible,
- el Teorema de Hahn-Banach,
- el Teorema de completud para la lógica de primer orden,
- toda álgebra de Boole es isomorfa a un campo de conjuntos,
- el producto de una familia infinita de espacios compactos es compacto,
- todo cuerpo tiene una clausura algebraica

y muchas otras. Es probable que el lector no conozca la mayoría de ellas, las incluimos para despertar su curiosidad y para mostrar la importancia que tiene este axioma en todas las áreas de la matemática y que sin el Axioma de Elección esta disciplina sería muy distinta.

4.4.3 Ejercicios

1. Demuestre, sin usar el Axioma de Elección, que todo conjunto finito de conjuntos no vacíos tiene una función de elección. (Indicación: Use inducción sobre el número de elementos del conjunto).
2. Demuestre que la siguiente proposición es equivalente al Axioma de Elección.

   Principio de Zermelo:

   Si P es una partición de un conjunto A, entonces existe $M \subseteq A$ que contiene un único elemento de cada bloque $B \in P$.

   Recordemos que toda partición sobre A induce una relación de equivalencia sobre A y cuyas clases de equivalencia son los elementos de P. El principio de Zermelo nos dice que podemos escoger un elemento de cada clase de equivalencia, es decir, un sistema de representantes de las clases de equivalencia.
3. Demuestre que toda relación binaria contiene una función con el mismo dominio.

4.5 APENDICE A: Equivalencias del Axioma de Elección: Demostraciones

4.5.1 El Lema de Zorn implica el Axioma de Elección

Sea A un conjunto no vacío de conjuntos no vacíos.

Definamos $K = \{F : \text{Dom } F \subseteq A\,, F(x) \in x\}$, es decir, funciones parecidas a una función de elección sólo que el dominio puede ser más pequeño. Obviamente si hubiera un elemento de K cuyo dominio es A, entonces habríamos terminado.

El conjunto K está ordenado por inclusión. Recordemos que dadas dos funciones F y G

$$F \subseteq G \text{ si y solo si } \text{Dom } F \subseteq \text{Dom } G \text{ y para } x \in \text{Dom } F\,,\ G(x) = F(x)\,,$$

o sea, G extiende a F.

Es también claro que K no es vacío. En efecto, si $B \in A$, como B no es vacío, existe $b \in B$. Consideramos $F = \{(B, b)\}$, entonces $F \in K$.

Sea entonces $C = \{F_i : i \in I\}$ una cadena de elementos de K. Entonces $F = \bigcup C$ es una función tal que $\text{Dom } F \subseteq \bigcup \text{Dom } F_i \subseteq A$. Además para cada $x \in \text{Dom } F$, $x \in \text{Dom } F_i$, para algún $i \in I$ y, por lo tanto, $F(x) = F_i(x) \in x$. Es decir $F \in K$, lo que demuestra que toda cadena tiene una cota superior en K.

Por el Lema de Zorn K tiene un elemento maximal F. Bastará con demostrar que $\text{Dom } F = A$ para que F sea una función de elección para A.

Supongamos que no es así. Entonces hay un $a \in A$ tal que $a \notin \text{Dom } F$. Como $a \neq \emptyset$, podemos formar $G = F \cup \{(a, b)\}$, donde $b \in a$. Es claro que $G \in K$, pero además $F \subsetneq G$, contradiciendo la maximalidad de F. Esto demuestra que $\text{Dom } F = A$ y, por lo tanto, que F es una función de elección para A. □

4.5.2 El Axioma de Elección implica el Lema de Zorn

El Lema de Zorn apareció por primera vez en los trabajos de K. Kuratowski en la década del 20, del siglo pasado. Su importancia radica en que es probablemente la manera más fácil y común de aplicar el axioma de elección en distintas ramas de la matemática. Esta es una variación de la demostración del Lema de Zorn que aparece en [**4**].

Supongamos que $(A, \leq)$ es un orden parcial en el cual toda cadena tiene una cota superior. Sea $\widetilde{A}$ el conjunto de todas las $\leq$–cadenas en A. Entonces $\widetilde{A}$ es un orden parcial bajo inclusión. Si $\mathcal{C}$ es una $\subseteq$–cadena en $\widetilde{A}$, entonces es claro que $\bigcup_{B\in\mathcal{C}} B$ es también una $\leq$–cadena en A. En efecto, si $x, y \in \bigcup_{B\in\mathcal{C}} B$, entonces $x \in C_1$ e $y \in C_2$ para ciertos C_1, $C_2 \in \mathcal{C}$. Pero $\mathcal{C}$ es una $\subseteq$–cadena, entonces o bien $C_1 \subseteq C_2$ o bien $C_2 \subseteq C_1$, digamos, sin pérdida de generalidad, que ocurre lo primero. Entonces x, $y \in C_2$ y como C_2 es una $\leq$–cadena, o bien $x \leq y$ o bien $y \leq x$, es decir, $\bigcup_{B\in\mathcal{C}} B$ es una $\leq$–cadena y, por lo tanto, pertenece a $\widetilde{A}$. Como el orden es la inclusión, es claro que $\bigcup_{B\in\mathcal{C}} B$ es una cota superior para $\mathcal{C}$ en $\widetilde{A}$.

Más aún, si $\widetilde{A}$ tiene un elemento $\subseteq$–maximal, entonces también A tiene un elemento maximal. Para demostrarlo, supongamos que M es una $\leq$–cadena maximal, entonces cualquier cota superior m de M debe pertenecer a M, o si no, $M \cup \{m\}$ sería una cadena más grande. Por lo tanto, m es el mayor elemento de M y, en particular, m es la única cota superior de M y, por lo tanto, m es maximal en A.

Basta entonces probar que $\widetilde{A}$ tiene un elemento maximal para concluir nuestra demostración. Eso haremos ahora.

Consideremos para cada $a \in \widetilde{A}$ el conjunto B_a de todas las cotas superiores de a. Por hipótesis $B_a \neq \emptyset$. Si una cota superior no pertenece a la cadena a, entonces podemos extender la cadena y, por lo tanto, a no es maximal. Luego, la cadena a es maximal si y solo si $B_a \subseteq a$, es decir, si no hay cotas superiores que no pertenezcan a la cadena.

Supongamos que no hay cadenas maximales. Esto es equivalente a suponer que para todo $a \in \widetilde{A}$, $B_a - a \neq \emptyset$. Sea f una función de elección sobre $\{B_a - a : a \in \widetilde{A}\}$, es decir, para cada $\leq$–cadena a en $\widetilde{A}$, $f(B_a) \in B_a$, luego $f(B_a)$ es una cota superior de a que no pertenece a a.

Para cada $a \in \widetilde{A}$ definamos $a^+ = a \cup \{f(B_a)\}$.

Diremos que un subconjunto $\mathcal{N} \subseteq \widetilde{A}$ es cerrado, si verifica las tres propiedades de clausura: (i) $\emptyset \in \mathcal{N}$ (ii) Si $a \in \mathcal{N}$, entonces $a^+ \in \mathcal{N}$. (iii) Si $\mathcal{C}$ es una cadena en $\mathcal{N}$, entonces $\bigcup_{B \in \mathcal{C}} B$ está en $\mathcal{N}$.

Notemos que $\widetilde{A}$ mismo es cerrado ya que para cada a, a^+ es una cadena y como vimos anteriormente, una unión de cadenas es una cadena. Además, es inmediato que la intersección de un conjunto de conjuntos cerrados es cerrada. En particular, la intersección $\mathcal{M}$ de todos los conjuntos cerrados es cerrada; $\mathcal{M}$ es entonces el conjunto cerrado más pequeño, es decir, está contenido en todo conjunto cerrado.

Diremos que un elemento $C \in \mathcal{M}$ es $\subseteq$–comparable si para todo $A \in \mathcal{M}$ o bien $A \subseteq C$ o bien $C \subseteq A$. Queremos demostrar que todos los elementos de $\mathcal{M}$ son $\subseteq$–comparables. Esto implicará que $\mathcal{M}$ es una cadena.

Lema 4.10. *Supongamos que C es $\subseteq$–comparable. Si $a \in \mathcal{M}$ y $a \subsetneq C$ entonces $a^+ \subseteq C$.*

Demostración. Supongamos que $a^+ \not\subseteq C$. Entonces $C \subsetneq a^+$. Pero entonces $a \subsetneq C \subsetneq a^+$, lo que contradice el que a^+ se construyó adjuntando a a un único elemento de A. □

Lema 4.11. *Supongamos que C es $\subseteq$–comparable, y sea $\mathcal{N} = \{a \in \mathcal{M} : a \subseteq C \text{ ó } C^+ \subseteq a\}$.*

Entonces $\mathcal{N}$ es cerrado y, por lo tanto, $\mathcal{N} = \mathcal{M}$.

Demostración. Dado $a \in \mathcal{N}$ tenemos $a \subsetneq C$, $a = C$, ó $C^+ \subseteq a$. En el primer caso, $a^+ \subseteq C$ por el lema anterior, luego $a^+ \in \mathcal{N}$; en los otros casos, $C^+ \subseteq a \subseteq a^+$, y también $a^+ \in \mathcal{N}$. Esto demuestra que la segunda propiedad de clausura se satisface.

En seguida, supongamos que $\mathcal{C}$ es a cadena en $\mathcal{N}$, y sea $D = \bigcup_{B\in\mathcal{C}} B$. Si todo $B \in \mathcal{C}$ es subconjunto de C, entonces $D \subseteq C$, luego $D \in \mathcal{N}$. Si no, algún $B \in \mathcal{C}$ contiene a C^+; entonces $C^+ \subseteq D$, y nuevamente $D \in \mathcal{N}$, por lo que también se cumple la tercera condición. La primera se cumple trivialmente. □

Por último, consideremos el conjunto de los elementos $\subseteq$–comparables de $\mathcal{M}$. Probaremos que este conjunto es cerrado, por lo tanto, es todo $\mathcal{M}$. Si C es $\subseteq$–comparable y $a \in \mathcal{M}$, entonces por el segundo lema, o bien $a \subseteq C$ o bien $C^+ \subseteq a$. En cualquier caso a es comparable con C^+, luego C^+ es un conjunto $\subseteq$–comparable, es decir, se cumple la segunda condición de clausura. En seguida, supongamos que $\mathcal{C}$ es una cadena de conjuntos $\subseteq$–comparables y sea $D = \bigcup_{B\in\mathcal{C}} B$. Dado $a \in \mathcal{M}$, o bien $B \subseteq a$ para todo $B \in \mathcal{C}$, en cuyo caso $a \subseteq D$, o bien $a \subseteq B$ para algún $B \in \mathcal{C}$, en cuyo caso $a \subseteq D$. Luego D es comparable y el conjunto de los conjuntos $\subseteq$–comparables cumple la tercera condición de clausura, luego es efectivamente cerrado. La primera condición se cumple trivialmente.

Lo que hemos demostrado es que todos los elementos de $\mathcal{M}$ son $\subseteq$–comparables, o sea, $\mathcal{M}$ es una $\subseteq$–cadena en $\widetilde{A}$.

Consideramos ahora la unión de esta cadena, $U = \bigcup \mathcal{M}$. Como $\mathcal{M}$ es cerrado, por iii) $U \in \mathcal{M}$ y por ii) $U^+ \in \mathcal{M}$ luego $U^+ \subseteq U$, o sea $f(U) \in U$, pero esto es una contradicción, lo que implica que debe haber una cadena maximal. □

4.5.3 El Lema de Zorn implica el Principio de Buen Orden

Sea A un conjunto cualquiera y consideremos el siguiente conjunto

$$B = \{(C, \leq_C) : C \subseteq A \quad \text{y} \quad \leq_C \text{ es un buen orden de } C\}.$$

Es claro que B está bien definido porque $C \in \mathcal{P}(A)$ y $\leq_C \in \mathcal{P}(A \times A)$ para cualquier C. Este es un conjunto no vacío, por ejemplo, $\emptyset \in B$ porque $\emptyset$ no tiene subconjuntos no vacíos ($\leq_\emptyset = \emptyset$). Por supuesto, hay ejemplos menos triviales. Dado cualquier $a \in A$, hacemos $C = \{a\}$ y $\leq_C = \{(a, a)\}$. El lector podrá inventar otros más complicados.

El conjunto B está ordenado de la siguiente manera decimos que

$$(C, \leq_C) \preceq (D, \leq_D)$$

si y solo si

1. $C = \{x \in D : x \leq_D d \text{ para algún } d \in D\}$
2. $\leq_C \subseteq \leq_D$

Es decir, C es lo que a veces se llama un segmento inicial de D, o sea, todos los elementos más pequeños que un cierto elemento dado (por ejemplo en los números reales, un segmento inicial es un intervalo $(-\infty, a]$). En particular, esto implica que $C \subseteq D$. La segunda condición dice que el orden del conjunto más grande extiende al orden del conjunto más pequeño. Es claro que esto es un orden sobre B.

Consideremos ahora una cadena $\mathcal{B} = \{(C_i, \leq_{C_i}) : i \in I\}$ de elementos de B. Recuerde que los elementos de $\mathcal{B}$ son esencialmente subconjuntos bien ordenados de B cada vez más grandes.

Consideramos ahora el siguiente par

$$K = \bigcup\{C_i : i \in I\} \quad \text{y} \quad \leq_K = \bigcup\{\leq_{C_i} : i \in I\}.$$

Veremos que el par formado por estos conjuntos pertenece a B. Es claro que $K \subseteq A$. Habría que ver que $\leq_K$ es un buen orden. Para esto tomemos un subconjunto no vacío N de K. Como N no es vacío, podemos tomar un elemento $n \in N$. Entonces $n \in C_i$ para algún $i \in I$, por lo tanto, $N \cap C_i \subseteq C_i$ es no vacío y como C_i está bien ordenado, tiene un $\leq_{C_i}$–menor elemento n_i. Es claro que $n_i \in N$.

Probaremos ahora que n_i es el $\leq_N$–menor elemento de N. Si no lo fuera, existiría otro elemento $r \in N$ tal que $r \leq_N n_i$, pero $r \neq n_i$, es decir, es estrictamente menor que n_i en el orden $\leq_N$. Además $r \in C_j$ para algún $j \in I$.

Ahora recordamos que $\mathcal{B}$ es una $\preceq$–cadena, por lo tanto, o bien C_i es un segmento inicial de C_j o bien C_j es un segmento inicial de C_i. En cualquier caso tanto n_i como r pertenecen a uno de los dos conjuntos C_i o C_j y en ellos los órdenes respectivos $\leq_{C_i}$, $\leq_{C_j}$ y $\leq_N$ coinciden, de tal manera que si $r \leq_N n_i$, tendríamos que $r \leq_{C_i} n_i$, lo que es una contradicción.

Lo que acabamos de demostrar es que $(K, \leq_K)$ es una cota superior de $\mathcal{B}$. Por lo tanto, aplicando el Lema de Zorn, B tiene un elemento maximal $(M, \leq_M)$. Resta por demostrar que $M = A$ y tendremos el buen orden requerido.

Supongamos que $M \neq A$ y sea $a \in A - M$. Entonces, definimos $C = M \cup \{a\}$ y extendemos el orden $\leq_M$ agregando a al final, es decir, hacemos

$$\leq_C = \leq_M \cup \{(m, a) : m \in M\}.$$

Es fácil ver que éste es un buen orden sobre C que extiende al orden de M y que M es un segmento inicial de C, por lo tanto, $(M, \leq_M) \prec (C, \leq_C)$ y, por lo tanto, $(M, \leq_M)$ no es un elemento maximal, contrario a nuestra elección. □

4.5.4 El Principio de Buen Orden implica el Axioma de Elección

Sea A un conjunto de conjuntos no vacíos. Por el Principio de Buen Orden, cada uno de ellos está bien ordenado. Dado $a \in A$ sea m_a el menor elemento de A según ese orden. Definimos

$$\begin{array}{rcl} F : A & \longrightarrow & \bigcup A \\ a & \longmapsto & m_a \end{array}$$

Esta es una función de elección para A. □

4.5.5 El Lema de Zorn implica el Principio de Tricotomía

Sean A, B conjuntos. Definimos

$$R = \{f \,:\, \text{Dom } f \subseteq A\,,\ \text{Rec } f \subseteq B\,,\ f \quad \text{inyectiva}\}\,.$$

Es claro que R es un orden parcial. Como en los ejemplos anteriores, vemos que si $\mathcal{B}$ es una cadena, entonces $\bigcup \mathcal{B}$ es una cota superior.

Por el Lema de Zorn existe una función maximal F. Supongamos que $\text{Dom } F \neq A$ y $\text{Rec } F \neq B$. Entonces existe $a \in A - \text{Dom } F$ y $b \in B - \text{Rec } F$.

Definimos

$$G = F \cup \{(a, b)\}\,.$$

Entonces, G es inyectiva, $\text{Dom } G \subseteq A$ y $\text{Rec } G \subseteq B$, o sea, T no es maximal lo que es una contradicción. Por lo tanto, o bien $\text{Dom } F = A$ o bien $\text{Rec } F = B$. En el primer caso F es inyectiva de A en B, en el segundo caso, F^{-1} es inyectiva de B en A. □

4.5.6 El Principio de Tricotomía implica el Principio de la Imagen Inversa

Sean A y B conjuntos no vacíos. Supongamos sin pérdida de generalidad que existe una función inyectiva, $f : A \longrightarrow B$. Sea $a \in A$ y definamos

$$g : B \longrightarrow A$$

$$g(x) = \begin{cases} f^{-1}(x) & , \text{ si } \quad x \in f[A], \\ a & , \text{ si } \quad x \in B - f[A]. \end{cases}$$

Entonces g es sobreyectiva. □

Correspondería ahora demostrar que el Principio de la Imagen Inversa implica el Axioma de Elección, cerrando así el ciclo que demostraría la equivalencia de todos ellos. Sin embargo, esta demostración requiere del desarrollo de la teoría de números ordinales, lo que escapa el alcance de este libro. De la misma manera, tampoco podemos demostrar la equivalencia de **AC** con el importante Principio del Buen Orden. El lector interesado encontrará estas demostraciones en [**3, 8, 10**].

4.5.7 Ejercicios

1. Demuestre que el conjunto K definido en el Teorema 4.6, Principio de Zermelo implica AC, es efectivamente un conjunto y que el conjunto P es una partición de K.
2. Proporcione los detalles que demuestran que la relación R definida en la demostración del Teorema 4.6, Principio de Kuratowski implica Principio de Tricotomía, es efectivamente un orden parcial.
3. Compruebe que la relación definida en 4.5.3 es efectivamente un orden.
4. Compruebe que el conjunto $\bigcup \mathcal{B}$ definido en 4.5.5 es una cota superior de la cadena $\mathcal{B}$.

4.6 APENDICE B: Formalización

Para un estudio formal de la Teoría Axiomática de Conjuntos se hace necesario definir la noción de propiedad en términos de la lógica subyacente, esto es de la lógica clásica. A continuación definiremos este concepto.

Como dijimos anteriormente, lo que queremos evitar con esto son definiciones de conceptos vagos o inaplicables. Nos limitaremos entonces a expresiones que se pueden escribir en forma precisa, con los símbolos estrictamente necesarios para el propósito. Sólo estas expresiones serán aceptables en nuestra teoría y representarán propiedades u otras entidades.

El lenguaje formalizado está constituido por un conjunto de símbolos básicos y por reglas que nos permiten formar expresiones más complicadas, a partir de esos símbolos originales. Recordemos que nuestra única noción primitiva es la de pertenencia, pero necesitamos también de la noción lógica de identidad o igualdad. Las expresiones de este lenguaje se llaman *fórmulas* y se construyen (de la manera usual en matemática) a partir de dos expresiones básicas $X \in Y$, y $X = Y$, donde X e Y son dos variables o constantes, no necesariamente distintas. La primera se lee X *pertenece* a Y y la segunda X *es igual a* Y. Su significado intuitivo es el obvio.

Usamos los conectivos lógicos: $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$, es decir, los símbolos usuales para la negación, disyunción, conjunción, implicación y equivalencia para formar las fórmulas complejas

$$\neg\varphi\,, \quad (\varphi \vee \psi)\,, \quad (\varphi \wedge \psi)\,, \quad (\varphi \rightarrow \psi)\,, \quad (\varphi \leftrightarrow \psi)\,.$$

También formaremos fórmulas cuantificadas $\forall x\varphi(x)$ y $\exists x\varphi(x)$. Estas se leen *cualquier conjunto* x verifica φ y *existe (por lo menos) un* conjunto x que verifica φ, respectivamente. Su significado es también evidente. Recordamos que los únicos objetos de nuestra teoría son los conjuntos, de tal manera que los cuantificadores nos hablan de conjuntos.

En general, escribimos $X \notin Y$ y $X \neq Y$ en lugar de $\neg(X \in Y)$ y $\neg(X = Y)$, respectivamente.

Si bien solamente aquellas expresiones obtenidas de esta manera son fórmulas, en la práctica aceptamos expresiones tales que es inmediato ver cómo se podrían escribir formalmente. También aceptamos símbolos auxiliares que han sido debidamente definidos, por ejemplo, $\subseteq$, $\emptyset$, $\cup$, $\cap$, etc., porque se pueden reemplazar fácilmente por su definición.

Ejemplos 4.12.

1. $\forall x\exists y(x \in y \wedge x \neq y)$ es una fórmula que dice que todo conjunto pertenece a algún conjunto diferente de él mismo. Ésta es una oración que resulta ser cierta en la teoría.
2. $\forall x(x \in X \rightarrow x \neq \emptyset)$, es una fórmula que define una propiedad. Un conjunto X que satisfaga esta oración es tal que sus elementos son no vacíos.

3. $x \in y \wedge \forall z(z \in y \to z = x)$. Esta fórmula es satisfecha por dos conjuntos x e y si y solo si $y = \{x\}$.

El primer ejemplo difiere de los otros en que todas las variables caen bajo la "influencia" de un cuantificador. Los lógicos llaman *oración* a este tipo de fórmula. En los otros dos ejemplos hay variables, X en el segundo, x e y en el tercero, que no están cuantificadas. Los lógicos les llaman *variables libres*.

Las expresiones con una sola variable libre representan las *propiedades* en nuestro lenguaje. Intuitivamente, si reemplazamos la variable libre de la fórmula por un conjunto, la oración resultante es cierta, decimos que el conjunto verifica la propiedad descrita. Aquellos que no la hacen verdadera, no gozan de la propiedad.

Análogamente, las fórmulas como en el tercer ejemplo, con exactamente dos variables libres, son satisfechas por pares de conjuntos y sirven para definir relaciones y funciones (binarias). Como vimos antes en el Axioma de Reemplazo, una propiedad $\varphi(x, y)$ con dos variables libres x e y es una función proposicional si para todo conjunto a existe un único conjunto b tal que $\varphi(a, b)$ se verifica. Ejemplos de éstas son las fórmulas $\varphi(x, y)$ siguientes:

$$y = \bigcup x\,, \quad y = \mathcal{P}(x)\,, \quad y = x \cup \{x\}\,, \quad y = x \cap a,$$

donde a es un conjunto fijo previamente definido, etc. Observemos que en rigor estas expresiones no corresponden a las estrictas normas de lenguaje que nos impusimos, sin embargo, todas ellas se pueden expresar de la manera correcta, por ejemplo, $y = \bigcup x$ corresponde a $\varphi(x, y) = \forall z(z \in y \leftrightarrow \exists u(z \in u \wedge u \in x))$.

Ejercicio 4.13. Escriba formalmente las funciones proposicionales

$$y = \bigcap x\,, \quad y = \mathcal{P}(x)\,, \quad y = x \cup \{x\}\,, \quad y = x \cap a\,.$$

Los axiomas en sus versiones formales son los siguientes.

A1. **Axioma de Extensionalidad:**

$$\forall X \forall Y(\forall z(z \in X \leftrightarrow z \in Y) \to X = Y)$$

A2. **Axioma de Separación:** Para cualquier propiedad $\varphi(x)$

$$\forall X \exists Y \quad \forall z(z \in Y \leftrightarrow (z \in X \wedge \varphi(x)))$$

A3. **Axioma del conjunto vacío:**

$$\exists X \forall x \quad x \notin X$$

A4. **Axioma de Pares:**

$$\forall X \forall Y \exists Z \ \ \forall x(x \in Z \leftrightarrow (x = X \vee x = Y))$$

A5. **Axioma de Uniones:**

$$\forall X\ \exists Y\ \forall z(z \in Y \leftrightarrow \exists u(z \in u\ \wedge\ u \in X))$$

A6. **Axioma del Conjunto Potencia:**[2]

$$\forall X\ \exists Y\ \forall z(z \in Y \leftrightarrow z \subseteq X))$$

A7. **Axioma del Conjunto Infinito:**

$$\exists X(\emptyset \in X \wedge \forall y(y \in X \rightarrow y \cup \{y\} \in X)\ )$$

A8. **Axioma de Reemplazo:** Si $\varphi(x, y)$ es una función proposicional,

$$\forall X \exists Y\ \ \forall y(y \in Y \leftrightarrow \exists x(x \in X \wedge \varphi(x, y)))$$

A9. **Axioma de Regularidad:**

$$\forall x(x \neq \emptyset \rightarrow \exists y\,(y \in x\ \wedge\ y \cap x = \emptyset\,))$$

[2]En rigor deberíamos escribir $\forall X\ \exists Y\ \forall z(z \in Y \leftrightarrow \forall u(u \in z \rightarrow u \in X))$, sin embargo, como la lectura de la fórmula se complica bastante y ya sabemos cómo definir $\subseteq$ usando sólo $\in$ y los símbolos lógicos, preferimos la escritura abreviada. Algo similar puede decirse del Axioma del Conjunto Infinito, en el que se usa unión y el conjunto $\{y\}$. Ambos se definen fácilmente.

Bibliografía

[1] Chuaqui, R., *¿Qué son los números?*, Editorial Universitaria, 1980.

[2] Dedekind, R., *Was sind und was sollen die Zählen?*, Brunswick, 1888.
Traducido al castellano en *¿Qué son y para qué sirven los números? y otros escritos*, Edición de J. Ferreirós. Madrid, Alianza, 1997. Ver también [**1**].

[3] Enderton, H. B., *Elements of Set Theory*, Academic Press, 1977.

[4] Halmos, P., *Teoría Intuitiva de los Conjuntos*, Editorial Continental, México, 1965.

[5] Hamilton, A. G., *Numbers, sets and axioms*, Cambridge University Press, 1982.

[6] Labra, A. , Suazo, A. *Elementos de la Teoría de Cuerpos*, J.C. Sáez Editor, Santiago, 2011.

[7] Lewin, R., *Introducción al Álgebra*, J.C. Sáez Editor, Santiago, 2011.

[8] Lewin, R., *Teoría Axiomática de Conjuntos*, Apuntes Facultad de Matemáticas, 1988, http://www.mat.puc.cl/∼rlewin

[9] Lewin, R., *¿Cuál es el primer natural?*, Revista del profesor de Matemáticas, Sociedad de Matemática de Chile, 1994, 1, 3–7.

[10] Monk, H. B., *Introduction to Set Theory*, McGraw–Hill, 1969.

[11] Moore, G., *Zermelo's Axiom of Choice, its origins development and influence*, Springer–Verlag, 1982.

[12] Peano, G., *Aritmetices Principia Nova Methodo Exposita*, Turín, 1889. (Traducido al inglés en Van Heijenoort [**14**], 83–97).

[13] Torretti, R., *El Paraíso de Cantor*, Editorial Universitaria, 1998.
(http://www.memoriachilena.cl/archivos2/pdfs/MC0031052.pdf)

[14] van Heijenoort, J., *From Frege to Gödel. A source book in Mathematical Logic, 1879–1931*, Cambridge, Harvard Univ. Press, 1967.

[15] Zermelo, E., *Beweiss, dass Jede Menge wohlgeordnet werden kann*, Matematische Annalen 1904, 59, 514–516. (Traducido al inglés en Van Heijenoort [**14**], 139–141).

[16] Zermelo, E., *Untersuchungen über die Grundlagen der Mengenlehre. I* , Matematische Annalen, 1908, 65, 261–281. (Traducido al inglés en Van Heijenoort [**14**], 199–215).

Índice Analítico

$\emptyset$, 25, 120
$\in$, 22
$\notin$, 22
$\subseteq$, 25
$\sharp A$, 104
ínfimo, 44

Axioma de Elección, 42, 105, 108, 113, 127
Axioma de Extensionalidad, 23, 119, 139
Axioma de Infinito, 58
Axioma de Pares, 26, 32, 120, 139
Axioma de Reemplazo, 37, 51, 122, 139, 140
Axioma de Regularidad, 123, 140
Axioma de Separación, 24, 26, 27, 29, 33, 36, 50, 119, 139
Axioma de Uniones, 27, 120, 140
Axioma del Conjunto Infinito, 121, 140
Axioma del Conjunto Potencia, 26, 121, 140
Axioma del Conjunto Vacío, 25, 120, 139
Axioma del Supremo, 100

buen orden, 48

cadena, P–cadena, 44
cardinal de un conjunto, 104
cardinalidad de un conjunto, 104
clase de equivalencia, 50
clases, 118
clases propias, 118
complemento relativo, 29
composición de funciones, 38
conjunto, 21
conjunto finito, 104
conjunto inductivo, 58
conjunto infinito, 104
conjunto numerable, 107
conjunto parcialmente ordenado, 43
conjunto potencia, 26, 121
conjunto totalmente ordenado, 43
conjunto transitivo, 62
conjunto vacío, 25, 120
conjuntos disjuntos, 27
conjuntos equinumerosos, 103
cortadura, 92
cortadura de Dedekind, 92

diferencia, 29
divisores del cero, 70, 80, 89, 100
dominio de una función, 36

elemento máximo, 44
elemento mínimo, 44
elemento maximal, 44
elemento minimal, 44
elementos, 22
enteros negativos, 77
enteros positivos, 77
equinumerosidad, 103

función, 36
función biyectiva, 37
función característica, 47
función creciente, 45
función de A en B, 36
función de elección, 127
función identidad, 41
función inyectiva, 37
función isótona, 45
función proposicional, 122, 139
función sobreyectiva, 37

función uno a uno, 37

hipótesis de inducción, H.I., 61
Hipótesis del continuo, 114

imagen de un conjunto por una función, 37
intersección, 27
inversa de una función, 38
inverso aditivo, 78
inverso aditivo(racionales), 87
inverso multiplicativo, 88

Lema de Zorn, 128
ley de tricotomía, 67

método diagonal de Cantor, 110

número irracional, 93
números enteros, 75
números naturales, 58
números racionales, 83
números reales, 93
neutro aditivo(racionales), 87
numerable, 107

orden denso, 85
orden discreto, 67
orden lineal, 42
orden total, 42

par no ordenado, 26
par ordenado, 32
partición, 50
pertenencia, 22, 138
Principio de Buen Orden, 127
Principio de Extensión de Órdenes, 130
Principio de Inducción, 61
Principio de Inducción Completa, 63
Principio de la Imagen Inversa, 128
Principio de Tricotomía, 128
Principio de Zermelo, 132
producto cartesiano, 33
producto de dos órdenes, 43
producto de enteros, 77
producto de números reales, 97
producto de racionales, 86

recorrido de una función, 36
relación, 35
relación compuesta, 38
relación de equivalencia, 49
relación de orden parcial, 42
relación inversa, 38
restricción de una función, 41

singleton, 26
subconjunto, 25
sucesor, 57
suma de enteros, 77
suma de números reales, 94
suma de racionales, 86
supremo, 44

unión, 27, 120